ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 7, Issue 6, June 2021

An Introductions Of Undetectable Keyloggers With Experimental Testing And Ethical Network Surveillance Using Packet Sniffing Tool

Ms.Vasuki S, Mr.R.Karthick

Assistant Professor

Computer Science and Engineering Department

Muthayammal Engineering College

Rasipuram, 637 408, India,

vasuki.s.cse@mec.edu.in

Poovarasan M, Sathishkumar M R, Vasanthpriyan R
Final year Students

Computer Science and Engineering Department

Muthayammal Engineering College

Rasipuram, 637 408, India

ABSTRACT: A Key Logger is an equipment gadget or a product program that records the ongoing action of a PC client, including the console keys, they press. This venture exhibits the model of a C# based, programming key logger. This records the keystrokes of the framework, for each particular time span, and sends it to the maker, without the information on the client. These sort of utilizations discover their use in IT tech parks and instructive foundations, to screen the dubious workers' and understudies' .Packet sniffing is a strategy for tapping every bundle as it streams across the organization; i.e., it is a procedure where a client sniffs information having a place with different clients of the organization. Parcel sniffers can work as a managerial device or for malevolent purposes. It relies upon the client's purpose. Organization directors use them for checking and approving organization traffic. Bundle sniffers are fundamentally applications. They are programs used to peruse parcels that traverse the organization layer of the Transmission Control Protocol/Internet Protocol (TCP/IP) layer. (Essentially, the parcels are recovered from the organization layer and the information is deciphered.) Packet sniffers are utilities that can be effectively utilized for network administration. At a similar time, it can likewise be utilized for evil exercises. In any case, a client can utilize various methods to identify sniffers on the arrange and shield the information from sniffers. The method behind bundle sniffing on shared transport broadcast LANs is clarified.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 7, Issue 6, June 2021

Keywords: keyloggers ,C#, Packet Sniffing Tools, Packet Sniffer, Network Vulnerability, Network Analysis, Wire shark, TCP dump.

I. INTRODUCTION :

Keylogger gather datas and send it back to an outsider – regardless of whether that is a lawbreaker, law authorization or IT divisions. "Keyloggers are programming programs that influence calculation that screen console strokes through design acknowledgment and different procedures,". Keylogger are utilized as an instrument by aggressor to steel client's usernames and passwords in internet business, interpersonal organization, Mail administration and so on There are numerous security programming for distinguishing keyloggers and some strategy have present for managing them. In this paper we will show that keylogger can be imperceptible from security programming. We will make a keylogger and afterward will change the design of keylogger then test it against famous security programming on the planet. At definite we will show that numerous security programming can't recognize keyloggers. We will probably present this new test. Keylogger can equipment or programming based. Equipment based ones can a just settles between the con sole connector and the PC's port. Programming based ones can be entire applications or apparatuses intentionally utilized or downloaded, or malware accidental tainting a gadgets. Information caught by keylogger can be sent back to aggressors by means of email or transferring log information to predefined sites, data sets, or FTP workers. In the event that the keylogger comes packaged inside a huge assault, entertainers may basically distantly sign into a machine to download keystroke information. Keylogger can be put on machines in various manners. Actual lumberjacks require an individual to be genuinely present to be set on a machine, which means such assaults are more diligently (however not difficult) to accomplish, and bound to come from an insider danger. Remote console can likewise be sneak around on distantly. In former times Hardware Keylogger is more in IT park and Browsing focus to catch the Keystroke to screen the clients and utilizes keystrokes action.

Parcel sniffing is a strategy for tapping every bundle as it streams across the organization; A bundle sniffer otherwise called a bundle analyzer, convention analyzer or organization analyzer - is a piece of equipment or programming used to screen network traffic. Sniffers work by analyzing surges of information bundles that stream between PCs on an organization just as between arranged PCs and the bigger Internet. These parcels are proposed for - and addressed to - explicit machines, yet utilizing a bundle sniffer in "unbridled mode" permits IT experts, end clients or pernicious gatecrashers to look at any bundle, paying

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 7, Issue 6, June 2021

little heed to objective. It's feasible to arrange sniffers twoly. The first is "unfiltered," which means they will catch all parcels conceivable and think of them to a neighborhood hard drive for later assessment.

Next is "sifted" mode, which means analyzers will just catch parcels that contain explicit information component. Parcel sniffers can work as a regulatory device or for noxious purposes. It relies upon the client's goal. Organization executives use them for observing and approving organization traffic. Parcel sniffers are fundamentally applications. They are programs used to peruse parcels that traverse the organization layer of the Transmission Control Protocol/Internet Protocol (TCP/IP) layer. (Essentially, the bundles are recovered from the organization layer and the information is deciphered.) Packet sniffers are utilities that can be proficiently utilized for network organization. Simultaneously, it can likewise be utilized for odious exercises. Notwithstanding, a client can utilize various methods to distinguish sniffers on the arrange and shield the information from sniffers. The method behind bundle sniffing on shared transport broadcast LANs is clarified. To see how a parcel sniffer functions, you need to initially comprehend that information goes through an organization as bundles. In bundle exchanged organizations, the information to be sent is separated into a few parcels. These bundles are reassembled once all the information parcels arrive at their expected objective.

OUR RESEARCH ABOUT UNDETECTABLE KEYLOGGERS

We utilized a keylogger that is composed with C# language on the grounds that numerous programmer use it and have many capacity that reasonable for this work, for example, interfacing with mail administrations. For encoding the source codes and string we will utilize brilliant get together and Multimedia Builder. Shrewd gathering is well known programming in encoding area. For testing the degree of encoding we will test keylogger with Bin Text Tools that it extricate all content from any record and we can see un-encoded text and for conclusive testing the keylogger again famous antivirus we utilize online labs like Jotti and VirusTotal.

II. BYTECODE ALGORITHM

Base64 is an encoding calculation that permits you to change any characters into a letter set which comprises of Latin letters, digits, furthermore, and cut.

Base64,In programming, Base64 is a gathering of double to-message encoding plans that address parallel information (all the more explicitly, an arrangement of 8-bit bytes) in an ASCII string design by

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 7, Issue 6, June 2021

making an interpretation of the information into a radix-64 portrayal. The term Base64 starts from a particular MIME content exchange encoding. Each non-last Base64 digit addresses precisely 6 pieces of information. Three 8-cycle bytes can along these lines be addressed by four 6-bit Base64 digits.Base64 is intended to convey information put away in twofold arrangements across channels that just dependably support text content. Base64 is especially predominant on the World Wide Web where its uses incorporate the capacity to insert picture records or other paired resources inside literary resources.

Source	Text(ASCII)	M				a				n					
	Octets	77(0x4d)				97(0x61)				110(0x6e)					
Bits		0	1	0	0	1	1	0	1	0	1	1	0	0	0	0	1	0	1	1	1	1	0
Base64 encoded	Sextets	19				22				5				46									
	character	T				W				F				u									
	Octets	84(0x54)				87(0x57)				70(0x46)				117(0x75)									

Base64 implementation uses A–Z, a–z, and 0–9 for the first 62 values.

Input		Output		Padding
Length	Text	Length	Text	
20	Any carnal pleasure.	28	QW55IGNhcm5hbCBwbGVhc3VyZS4=	1
19	Any carnal pleasure	28	QW55IGNhcm5hbCBwbGVhc3VyZQ==	2
18	Any carnalpleasur	24	QW55IGNhcm5hbCBwbGVhc3Vy	0
17	Any carnal pleasu	24	QW55IGNhcm5hbCBwbGVhc3U=	1
16	Any carnal pleas	24	QW55IGNhcm5hbCBwbGVhcw==	2

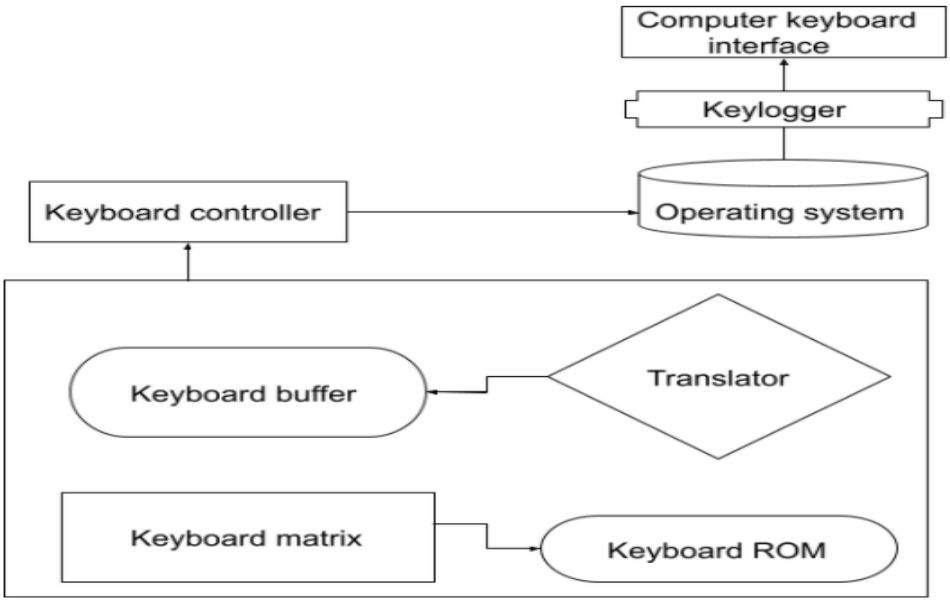
ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 7, Issue 6, June 2021

Example of String to base64 conversion

The reason for encoding is to change information so it tends to be appropriately (and securely) devoured by an alternate kind of framework, for example Twofold information being sent over email, or review unique characters on a page. The objective isn't to stay discreet, but instead to guarantee that it's ready to be appropriately devoured. Base64 is a six-digit encoding, and on the grounds that the decoded values are partitioned into 8-cycle octets on a cutting edge PC, each four characters of Base64-encode text (4 sextets = 4*6 = 24 pieces) addresses three octets of unencoded text or information (3 octets = 3*8 = 24 pieces). This implies that when the length of the unencoded input is certifiably not a different of three, the encode quote changes the yield cushioning yield should have cushioning added so its length is a various of four. The cushioning character is =, which shows that no further pieces are expected to completely encode the information.

III. KEYLOGGER ARCHITECTURE



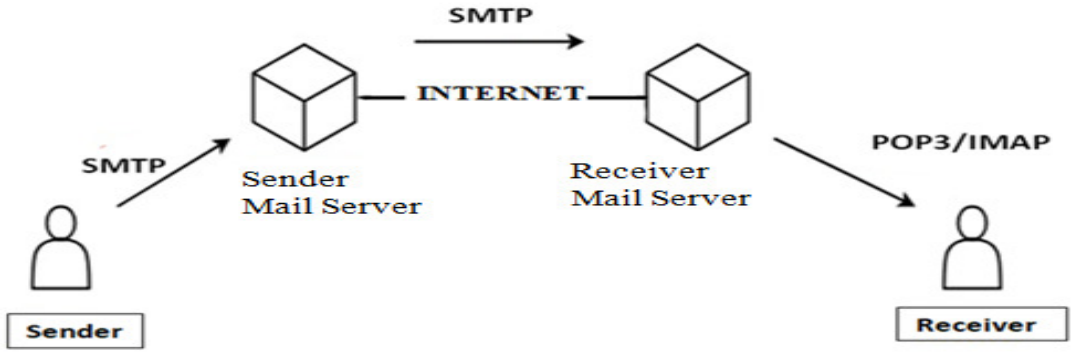
Form grabbing-based keylogger log Web form submission by record form data on submit events. This happen when the user complete a form and submit it, usually by clicking a button or pressing enter. This types of keyloggers records form datas before it is passed over the Internet. Once the log file is created, it is transmitted through email, to specified email id, with default subject and email body, which can be modified at the source.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

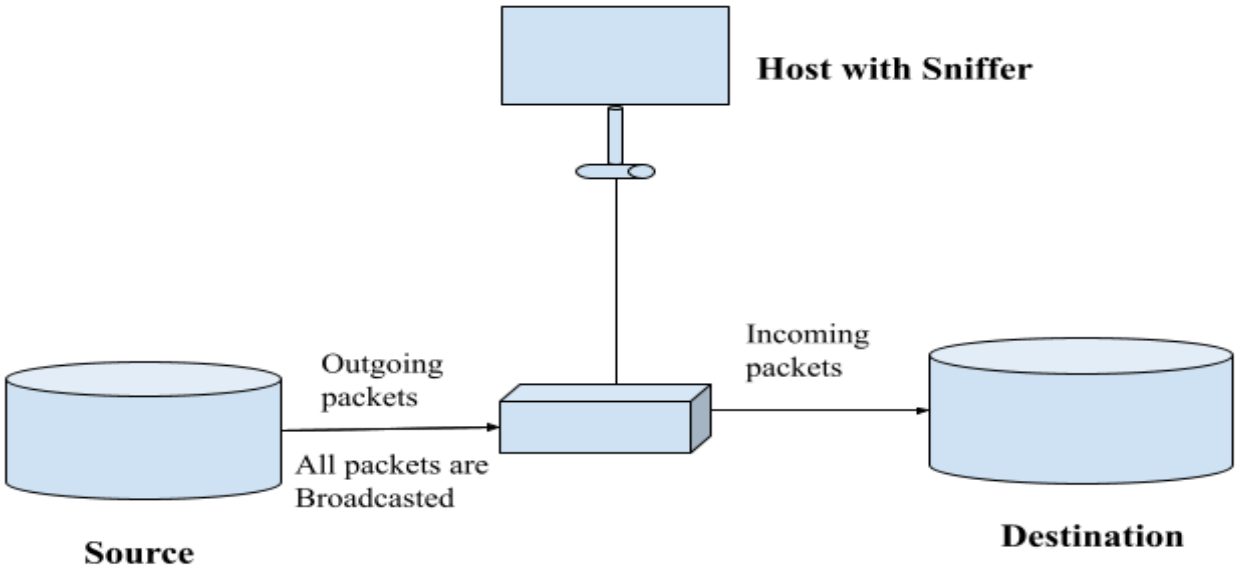
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 7, Issue 6, June 2021

IV. SMTP ARCHITECTURE

A large portion of the web frameworks use SMTP as a strategy to move mail starting with one client then onto the next. SMTP is a push convention and is utilized to send the mail though POP (mailing station convention) or IMAP (web message access convention) are utilized to recover those sends at the collector's side. SMTP is an application layer convention. A SMTP (Simple Mail Transfer Protocol) worker is an application that is basic role is to send, get, and additionally hand-off active mail between email senders and beneficiaries. At the point when you send an email, the SMTP worker measures your email, chooses which worker to send the message to, and transfers the message to that worker.



V. PACKET SNIFFINGARCHITECTURE



In the above chart, the source begin to send the message through the switch, in Transfer Layer all message send by the source is changed over into the parcels and in Network Layer the source MAC Address and

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 7, Issue 6, June 2021

objective MAC Address too likewise source IP Address and Destination IP Address are allocated in the bundle header. At that point it sends the bundles to the switch, Now the switch Broadcast every one of the parcels to every one of the machines. We need to turn on the wanton mode in our framework to tune in to the bundles that they move with which objective IP Address. Here our bundle sniffer begin tuning in and gather all the approaching and active association. It catch all the traffic going across the organization.

By definition, bundle sniffing is the way toward gathering information parcels that are sent across the organization. It doesn't rely upon the host or target parcel addresses. All things being equal, it centers around recovering information from the discussion. More often than not, bundles comprise of a subset of a lot more parcels. These parcels convert into pivotal snippets of data for the sniffer. Parcel sniffing is likewise completed by network heads. They sniff information bundles to take in additional about the rush hour gridlock from their private and got network channels.

VI. PACKET SNIFFERS:

1)TYPES OF SNIFFING

There are two kinds of sniffing-dynamic and aloof. As the name recommends, dynamic includes some action or association by the aggressor to acquire data. In detached the aggressor is simply covering up lethargic and getting the data. At the point when a bundle sniffer is introduced in the organization, the sniffer blocks the organization traffic and catches the crude information parcels. Therefore, the caught information parcel is dissected by the bundle sniffing programming and introduced to the organization director/expert in an easy to understand design. By easy to use, we mean the Network Administrator ought to have the option to figure out it.

2)PASSIVE SNIFFING

This sort of sniffing happens at the center. A center is a gadget that got the traffic on one port and afterward retransmits that traffic on any remaining ports. It doesn't consider that the traffic isn't intended for different objections. For this situation, assuming a sniffer gadget is put at the center point, all the organization traffic can be straightforwardly caught by the sniffer. The sniffer can stay there undetected for quite a while and spy on the organization. Since center points are not utilized nowadays a lot, this sort of assault will be an old fashioned stunt to perform. Centers are being supplanted by switches and that is the place where dynamic sniffing comes into the image.

3)ACTIVE SNIFFING

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

IJARMATE

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 7, Issue 6, June 2021

Basically, a switch learns a CAM table that has the Mac locations of the objections. Premise this table the switch can choose what organize bundle is to be sent where. In dynamic sniffing, the sniffer will flood the switch with fake demands so the CAM table gets full. When the CAM is full the switch will go about as a switch and send the organization traffic to all ports. Presently, this is genuine traffic that gets dispersed to every one of the ports. This way the assailant can sniff the traffic from the switch.

VII. SOURCE CODE OF PACKET SNIFFER

packetsniffer.py | main.py

```
import socket, sys, time, argparse
from struct import *


class Sniffer:
    def __init__(self):
        # argument parser for console arguments
        parser = argparse.ArgumentParser(
            description='A packet sniffer. Collect packets until ctrl+c pressed or after -t seconds ')
        # optimal arguments
        parser.add_argument("-f", "--filename", type=str, help="pcap file name (don't give extension)",
                            default='capture')
        parser.add_argument("-nr", "--noraw", action='store_false', default=True,
                            help="No Raw mode, Stops printing raw packets")
        parser.add_argument("-t", "--time", type=int, default=0, help="Capture time in second")
        # store pares arguments
        self.args = parser.parse_args()
        # initialize stat variables
        self.start_time = time.time()
        self.ip = False
        self.packet_count = 0
        self.tcp_count = 0
        self.udp_count = 0
        # try capture all packets(linux) if not, capture ip packets(windows)
        # windows doesnt support socket.AF_PACKET so fallback to ip packets
        try:
            # create raw packet socket
            self.s = socket.socket(socket.AF_PACKET, socket.SOCK_RAW, socket.ntohs(3))
        except AttributeError:
            # set ip mode true
            self.ip = True
```

VIII. NETWORK VULNERABILITY

The weakness is the shortcoming in the conventions, applications and information moved in the PC organizations. Subsequently, dangers abuse these shortcomings to harm assets, frameworks and applications. The primary thing that the aggressors do it is the surveillance of the casualty's organization framework by

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 7, Issue 6, June 2021

social affair weak data by utilizing apparatuses like burrow, whois, traceroute and nslookup just as bundle sniffing instruments. Organization filtering is utilized to discover weaknesses in the organization framework. Port sweep is the way toward tracking down the dynamic port when a customer demands the worker.

1)NETWORK SNIFFING

The organization sniffing is the way toward catching, observing, and examination of the information traffic going in the organization both approaching and active traffic. The device that played out this cycle is called bundle sniffer which is the program that caught traffic either in wired organization through the wired or remote organization by means of the air. Bundle sniffer has the advantages of dissecting the traffic, deciding and understanding the quality of the organization, conceivable pernicious and assaults, top use of transfer speed and its accessibility and tracking down the unstable applications, information and conventions.

IX. EXPERIMENTAL ANALYSIS AND FILTERING

The overall parcel sniffing measure is happened through three stages; first, the sniffer is assembled or caught the organization's data, second change of the caught twofold information into a coherent configuration, lastly applying examination and separating of the changed over information. There are different ways and strategies for separating and picking the predefined convention or some piece of information traffic. The NIC interface of the machine that the sniffing devices are introduced on it should be in unbridled mode to catch all parcels and casings on all portions of organization. This machine is called sniffer.

The separating cycle of the presently ongoing caught bundles or saved caught parcels is considered a significant for examination and analysis of different information traffic, conventions and applications that are utilized in the PC's organization framework. From that conventions like HTTP, ICMP, Domain Name System (DNS), TCP/IP, UDP, Simple Network Management Protocol (SNMP), and so forth, the entirety of the volume data and misfortunes of bundles are appeared in that caught data .

Moreover, these bundle sniffing apparatuses; TCPDump, Wireshark, and Colasoft are utilized for checking, examination, and reviewing of the information traffic on the PC networks either wired or remote organizations. Further, they are utilized in infiltration test and interruption identification by noticing unusual bundles in the organization. The organization's security dangers are appeared by sniffer in which has the capacity of catching all approaching and active information traffic, including the reasonable content client names and passwords, and other basic data.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 7, Issue 6, June 2021

X. TESTING SECURITY SOFTWARE'S AGAINST UNDETECTABLE KEYLOGGER

For testing security software against undetectable keyloggers, we use best antivirus according Av-Comparative report at March 2014 [10]. The participated antivirus in At Av-Comparative test have shown below.

AhnLab V3 Internet Securiy 8.0.8.2

- Avast! Free Antivirus 2014.9.0.2013
- AVG Internet Security 2014.0.4335
- AVIRA Internet Security 14.0.3.350
- Baidu Antivirus 4.0.9.57999 (EN)
- Bitdefender Internet Security 17.26.0.1106
- BullGuard Internet Security 14.0.278.3
- eScan Internet Security 14.0.1400.1572
- Emsisoft Anti-Malware 8.1.0.40
- ESET Smart Security 7.0.302.26
- F-Secure Internet Security 14.99.103
- Trend Micro Titanium Internet Security 7.0.1206
- Fortinet FortiClient 5.0.8.344
- Kaspersky Internet Security 14.0.0.4651 (e)
- Kingsoft Internet Security 2013.SP6.0.030511
- Lavasoft Ad-Aware Free Antivirus+ 11.1.5354.0
- McAfee Internet Security 16.8.708
- Microsoft Security Essentials 4.4.304.0
- Panda Cloud Free Antivirus 2.3.0
- Qihoo 360 Internet Security 4.9.0.4109 (EN)
- Sophos Endpoint Security and Control 10.3.1

XI. REQUIREMENTS:

1)HARDWARE REQUIREMENT

- 1 GB RAM

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 7, Issue 6, June 2021

- Pentium Core
- Wireless Adapter (WIFI)
- Physical Keyboard
- RJ45 cable

2)SOFTWARE REQUIREMENT

- Browsers : chrome , FireFox,etc.,
- IDE:Code block, python IDE
- OS:Windows 7

3)TOOL NAME:

UNDEDECTABLE KEYLOGGER &PACKET SNIFFER

4)STEP BY STEP PROCESS:

- Keystroke Module
- Timestamp Module
- Time Interval Module
- Encryption & Decryption Module
- Packets dumping module
- GeoIP Module

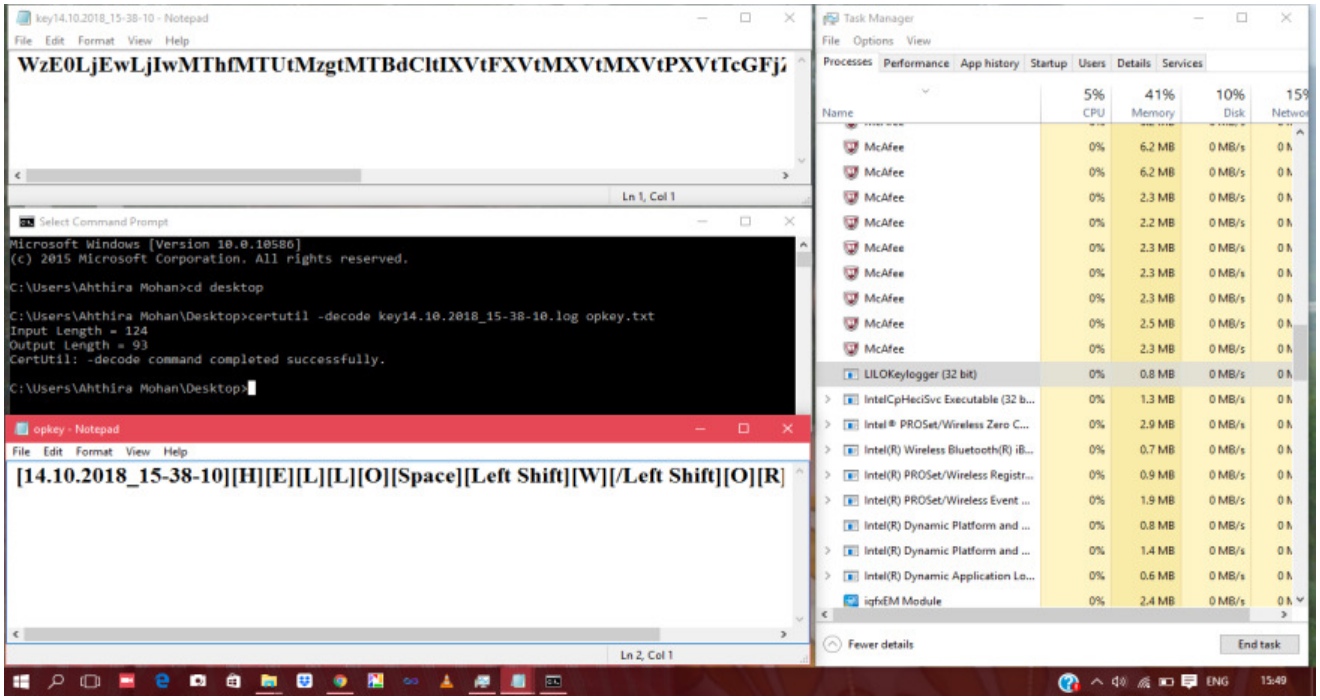
XII. CODE RUNNING IMAGE

1) **KEYLOGGER**

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

IJARMATE

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 7, Issue 6, June 2021



Output Fig For keylogger

2) PACKET SNIFFER

```
roshan@recon:~/Downloads$ sudo python model.py
[2020-06-18 13:09:07.434927]  ICMP-OUT:64 Bytes    IP-Version:4    SRC-MAC:80:c5:f2:54:2b:21    DST-MAC:a8:32:9a:04:43:22
    SRC-IP: 192.168.10.109    DST-IP:  172.217.160.206  Location:America/Los_Angeles
[2020-06-18 13:09:07.465226]  UDP-OUT:31 Bytes     SRC-MAC:80:c5:f2:54:2b:21    DST-MAC:a8:32:9a:04:43:22    SRC-PORT:5376
5    DST-PORT:53    SRC-IP:192.168.10.109    DST-IP:1.1.1.1  Location:None
[2020-06-18 13:09:07.507321]  UDP-IN:106 Bytes     SRC-MAC:a8:32:9a:04:43:22    DST-MAC:80:c5:f2:54:2b:21    SRC-PORT:53
  DST-PORT:53765    SRC-IP:1.1.1.1    DST-IP:192.168.10.109  Location:None
[2020-06-18 13:09:07.533521]  UDP-OUT:31 Bytes     SRC-MAC:80:c5:f2:54:2b:21    DST-MAC:a8:32:9a:04:43:22    SRC-PORT:5407
9    DST-PORT:53    SRC-IP:192.168.10.109    DST-IP:1.1.1.1  Location:None
[2020-06-18 13:09:07.568339]  UDP-IN:106 Bytes     SRC-MAC:a8:32:9a:04:43:22    DST-MAC:80:c5:f2:54:2b:21    SRC-PORT:53
  DST-PORT:54070    SRC-IP:1.1.1.1    DST-IP:192.168.10.109  Location:None
[2020-06-18 13:09:07.596866]  UDP-OUT:31 Bytes     SRC-MAC:80:c5:f2:54:2b:21    DST-MAC:a8:32:9a:04:43:22    SRC-PORT:5487
9    DST-PORT:53    SRC-IP:192.168.10.109    DST-IP:1.1.1.1  Location:None
[2020-06-18 13:09:07.618643]  ICMP-IN:64 Bytes    IP-Version:4          SRC-MAC:a8:32:9a:04:43:22    DST-MAC:80:c5:f2:54:
2b:21    SRC-IP: 172.217.160.206    DST-IP:  192.168.10.109  Location:America/Los_Angeles
```

Output Fig For Packet Sniffer

XIII. CONCLUTION:

In this paper we talk about the issue of keyloggers and .we show that keyloggers can be imperceptible from Up-to-date antivirus and hostile to adware apparatus and existing strategy can be fall flat against

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 7, Issue 6, June 2021

cutting edge keyloggers. We clarify stage and assignment of making of imperceptible keyloggers. We portray another test that should draw in by Antivirus Company's.

There are a few devices for catching, observing, evaluating and examination information traffic of PC networks both on wired and remote organizations and called bundle sniffing instruments. Bundle sniffing instruments work in three stages; assortment of information traffic from PC network in a crude double information, at that point convert the twofold information into intelligible organization and after that separating and examination of gathered information. The reason for bundle sniffing devices helps the organization heads to analyze the caught parcels showing the weaknesses and maltreatment of association's IT resources by workers. Just as, network security specialists and engineers need the parcel sniffing apparatuses for researching network security issues and investigating execution of correspondence conventions and organization's applications. Parcel sniffer is anything but a programmer's instrument. It is utilized to investigate, screen, break down and review the organization's information traffic to make the organization is protected, secure, dependable and expanding the presentation. In this examination, thought about between the three acclaimed parcel sniffing apparatuses; Wireshark, TCPDump, and Colasoft as per different boundaries, for example, interruption discovery capacity, upheld working frameworks, number of upheld conventions, open source code include, various interfaces, libpcap library, PCAP supporting, UI, unraveling structures, decided strange bundles, network correspondence in lattice map, and so forth It is utilized distantly through Telnet by clients and just backings TCP/IP convention. Those parcel sniffing devices need fostering the applications to work with the perception and supporting of more conventions examination in which perceiving the various pieces of the traffic. In future work, apply bundle sniffing devices on an assortment of uses, for example, Voice over IP (VoIP) and Video conferencing applications including examination and sifting strategies.

XVI. REFERENCES

[1] Nedhal A. Ben-Eid, Ethical Network Monitoring Using Wireshark and Colasoft Capsa as Sniffing Tools, International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 3, pp 471-478, March 2015.

[2] Palak Girdhar and Vikas Malik, A Study on Detecting Packet Using Sniffing Method, Journal of Network Communications and Emerging Technologies (JNCET) Vol. 6, Issue 7, July, 2016.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 7, Issue 6, June 2021

[3] Nabanita Mandal and Sonali Jadhav, A Survey on Network Security Tools for Open Source, IEEE, 2016.

[4] Savita Kamalakarrao Kulkarn, A Survey of Password Attacks, Countermeasures and Comparative Analysis of Secure Authentication Methods, IJARCSMS, Vol. 3, Issue 11, ppt. 319-331, November 2015.

[5] Dr. Aruna Varanasi, P. Swathi, Comparative Study of Packet Sniffing tools for HTTP Network Monitoring and Analyzing, IJCSET(www.ijcset.net), Vol. 6, Issue 12, pp. 406-409, December 2016.

[6] Oludele Awodele, Otusile Oluwabukola, A.C Ogbonna, and Ajayi Adebowale, Packet Sniffer – A Comparative Characteristic Evaluation Study, Proceedings of Informing Science & IT Education Conference (InSITE), pp. 91-100, 2015.

[7] ANSHUL GUPTA, A Research Study on Packet Sniffing Tool TCPDUMP, International Journal of Communication and Computer Technologies, Vol. 01, No. 49 Issue 06, pp. 172-174, July, 2013.

[8] Dr. Charu Gandhi, Gaurav Suri, Rishi P. Golyan, Pupul Saxena and Bhavya K. Saxena, Packet Sniffer – A Comparative Study, International Journal of Computer Networks and Communications Security, Vol.2, No. 5, ppt. 179–187, May 2014.

[9] Dr. Mahesh Kumar and Rakhi Yadav, TCP & UDP PACKETS ANALYSIS USING WIRESHARK, IJSETR, Vol. 4, Issue 7, ppt. 2470-2474, July 2015.

[10] Ajay Kumar, and Jai Bhagwan Yadav, Comparison: Wireshark on different parameters, International Journal Of Engineering And Computer Science, Vol. 5, Issue 3, ppt. 16041-16046, March 2016.

[11] Pallavi Asrodia and Hemlata Patel, Analysis of Various Packet Sniffing Tools for Network Monitoring and Analysis, International Journal of Electrical, Electronics and Computer Engineering, ppt. 55-58, 2012.

[12] Pallavi Asrodia, Mr. Vishal Sharma, Network Monitoring and Analysis by Packet Sniffing Method, International Journal of Engineering Trends and Technology (IJETT), Vol. 4, Issue. 5, ppt. 2133-2135, May, 2013.

[13] Inderjit Kaur, Harkarandeep Kaur, and Er. Gurjot Singh, Analysing Various Packet Sniffing Tools, International Journal of Electrical Electronics & Computer Science Engineering, Vol. 1, Issue. 5, ppt. 65-69, October 2014.

[14] Mohammed Abdul Qadeer, Mohammad Zahid, Arshad Iqbal and MisbahurRahman Siddiqui, Network Traffic Analysis and Intrusion Detection using Packet Sniffer, Second International Conference on Communication Software and Networks, ppt. 313-317, IEEE, 2010.

[15] Otusile Oluwabukola, Awodele Oludele, A.C Ogbonna, Ajeagbu Chigozirim, and Anyeahie Amarachi, A Packet Sniffer (PSniffer) Application for Network Security in Java, Issues in Informing Science and Information Technology, ppt. 389-400, Vol. 10, 2013.