Universidad Nacional Autónoma de México

Facultad de Ciencias – Ciencias de la Computación

Diseño de Interfaces de Usuario. Semestre 2019-2

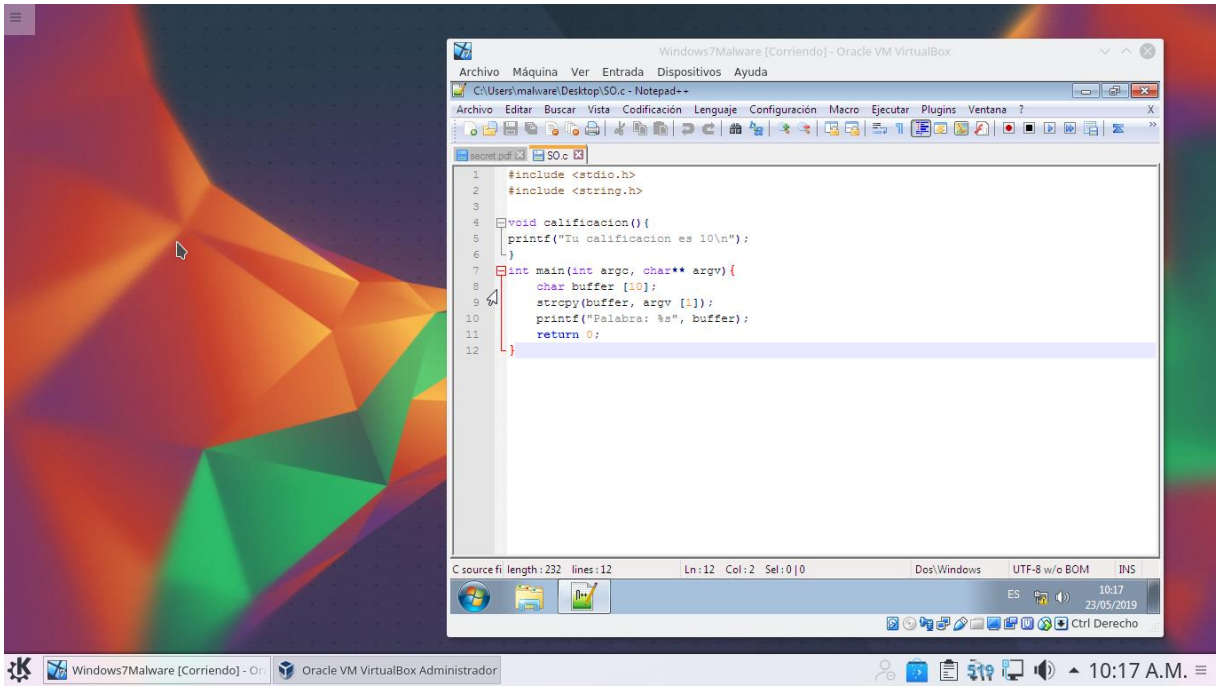
Estrada Gómez César Derian

Tarea 7

1. Reporte

Creamos una máquina virtual con el sistema operativo *Windows 7*.

Creamos un programa, *SO.c*, y escribimos el siguiente código:

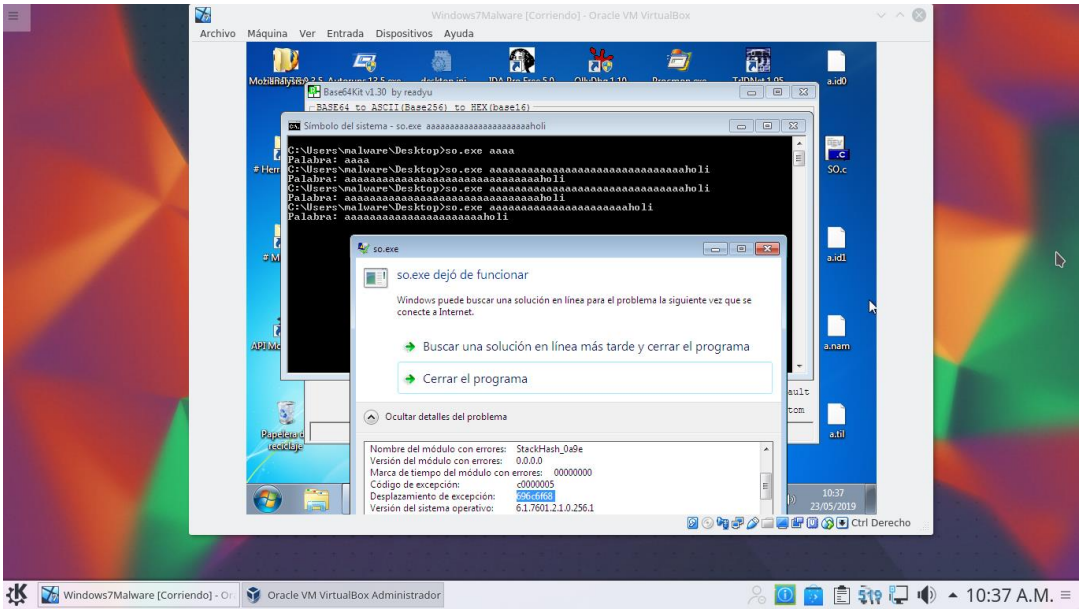


El programa recibe una cadena de no más 22 caracteres en *terminal*/*consola*.

Ejecutamos el programa:

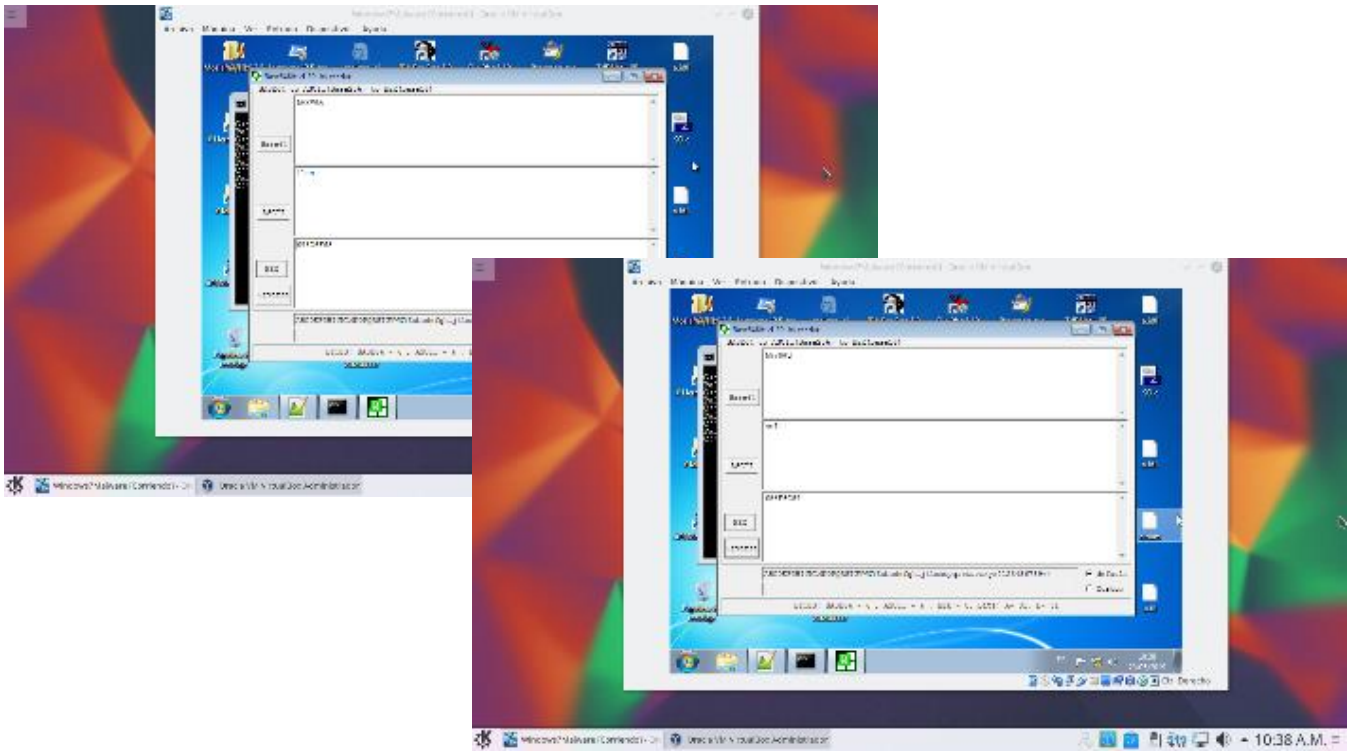
En las primeras dos ejecuciones, el programa se comporta cómo debería comportarse.

Sin embargo, en la tercera ejecución, al pasarle como parámetro: *aaaaaaaaaaaaaaaaaaaaholi*, ocurre lo siguiente:

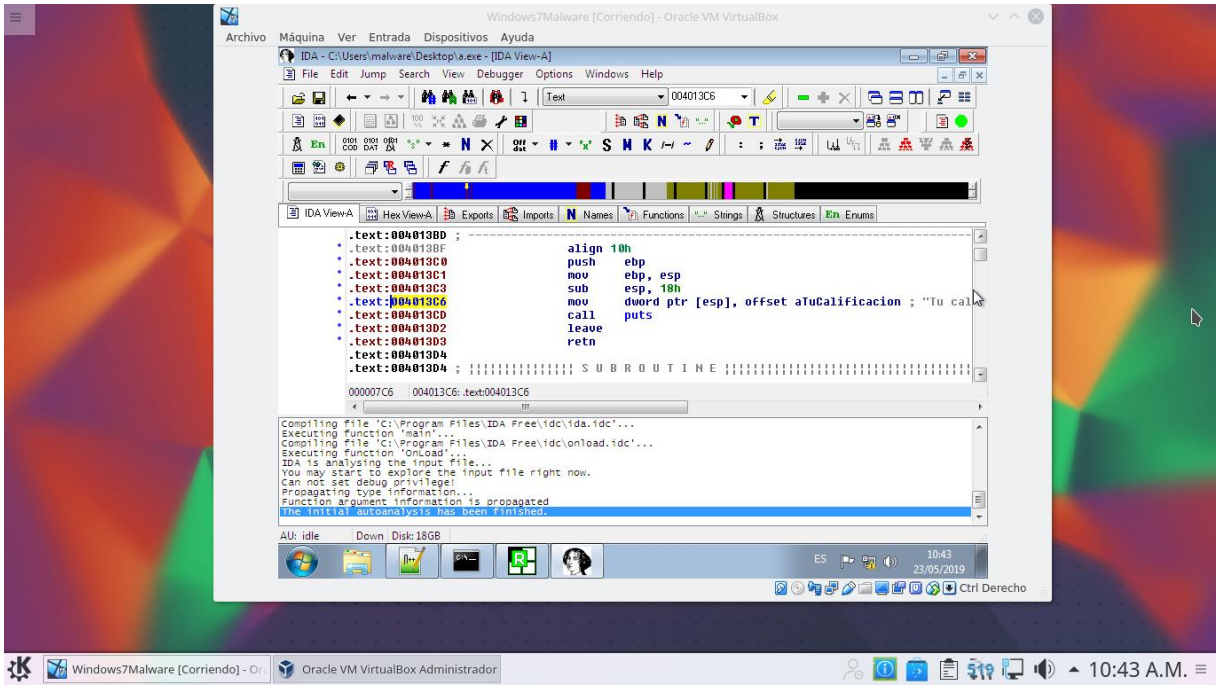


En el apartado *Desplazamiento de excepción*, se encuentra una línea en hexadecimal: **696c6f68**

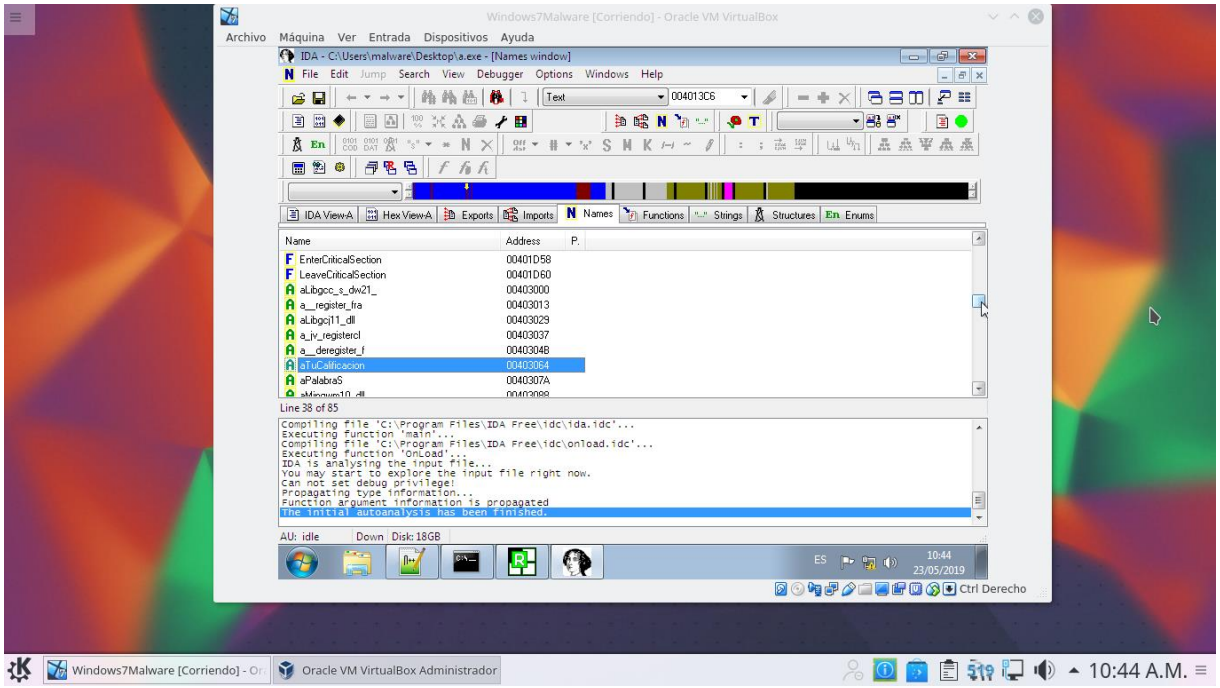
Por medio del programa *Base64*, le aplicamos *reversa* al texto anterior:



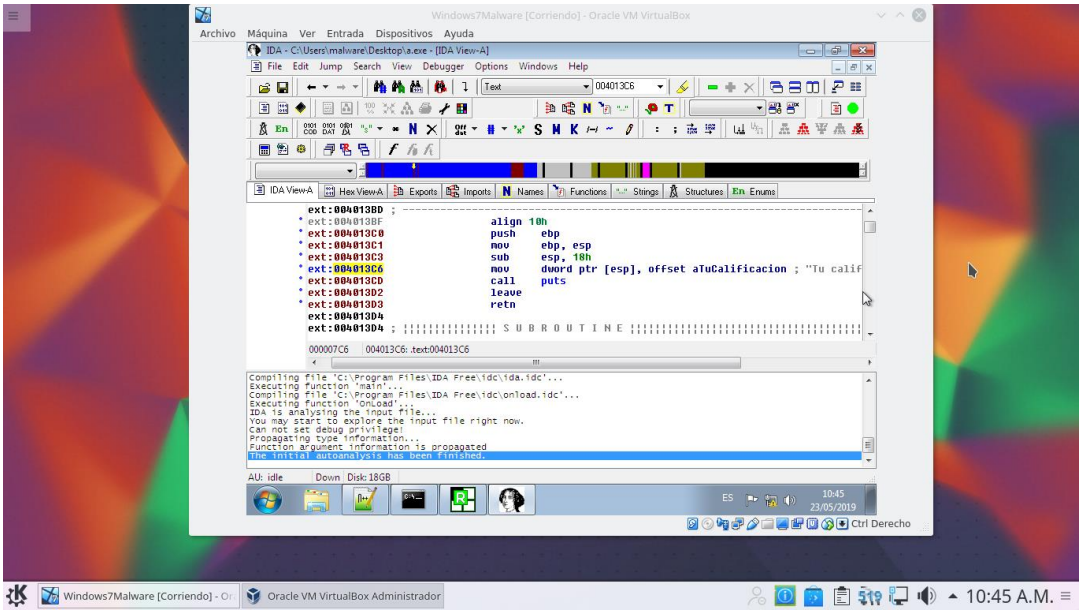
Ahora, en el programa *IDA* cargamos el programa *SO.c*



Nos dirigimos a la sección *Names*, y buscamos la línea 10 que aparece en nuestro código, *"…tu calificación…"* y damos doble clic



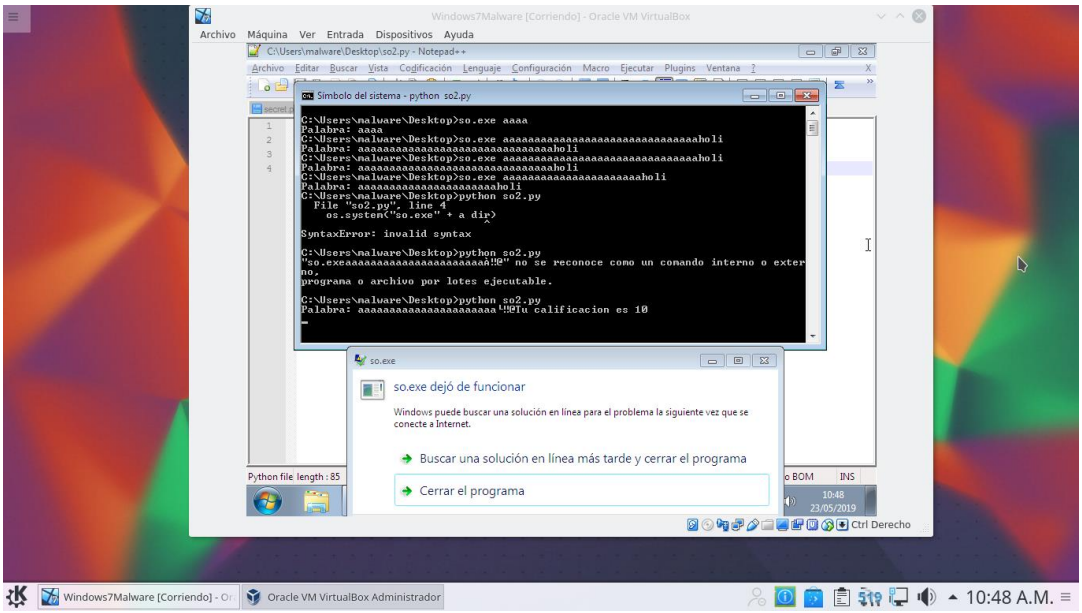
Copiamos el número de extensión: **004013C6**



Ahora, creamos el siguiente programa en *Python*.

```
so2.py
1  import os
2  a = "a"*22;
3  dir = "\xc0" + "\x13" + "\x40";
4  os.system("so.exe " + a + dir);
```

Por último, ejecutamos nuestro programa en python con el parámetro (*aaaaaaaaaaaaaaaaaaaaaholi*) con el cual el programa *SO.c* “tronó” la primera vez:



2. Preguntas

a) ¿Qué es *buffer overflow*?

Buffer overflow es una vulnerabilidad causada por la inserción de datos con tamaño superior al esperado por una aplicación, lo que provoca la sobreescritura de espacios adyacentes en la memoria.

b) Investiga acerca de algunas vulnerabilidades en la familia de sistemas operativos Windows

1. Windows 10 – Vulnerabilidad de Administrador de Montaje

Esta vulnerabilidad implica una posible escalada de privilegios al insertar un dispositivo USB en el sistema de destino. A través de este método, un atacante podría escribir un binario malicioso en el disco y ejecutar el código. Una actualización está disponible de Microsoft para parchar esta vulnerabilidad.

2. Windows – Vulnerabilidad de Microsoft Windows Journal

Esta vulnerabilidad podría permitir la ejecución remota de código si los usuarios abren un archivo *journal* especialmente diseñado.

3. Windows – Vulnerabilidad de Microsoft Font Driver

Windows Adobe Type Manager maneja incorrectamente las fuentes OpenType especialmente diseñadas, lo que puede resultar en una vulnerabilidad de ejecución remota de código. Esto puede hacer que los atacantes obtengan el control completo del sistema para instalar programas, ver / cambiar / eliminar datos y crear nuevas cuentas.

4. Windows 10 – Vulnerabilidad de Uso Compartido de Contacto de WiFi.

De forma predeterminada, Windows 10 comparte sus credenciales de WiFi a los contactos de Outlook, Skype y Facebook, probablemente para facilitar la compartición de WiFi y puntos de acceso. Esto hace posible que cualquiera de estos contactos se conecte a la red WiFi, si está cerca, sin autorización.

c) ¿Qué tipo de *buffer overflow* se vio en esta tarea?

En esta tarea se vio *Stack Buffer Overflow*. Cuando se ingresa una cantidad mayor de caracteres permitida por el límite del buffer, se crea un error que provoca que los caracteres restantes se escriban en direcciones contiguas de memoria.

d) ¿Qué tipo de actividad maliciosa pudiera realizarse con la vulnerabilidad de *buffer overflow*?

Se puede ejecutar código arbitrario, por ejemplo, código que apunte a una dirección en memoria donde inicie el código malicioso o, código que ya se encuentra en el espacio de direcciones del sistema, haciendo referencia a la dirección donde se encuentre localizado, por ejemplo, la ejecución de un Shell.

3. Referencias

1. **Revista Digital ".Seguridad". UNAM CERT**. https://revista.seguridad.unam.mx/numero23/uno-de-los-clsicos-buffer-overflow
2. ***Top 10 Windows 10 Vulnerabilities*. UpGuard™**. https://www.upguard.com/articles/top-10-windows-10-security-vulnerabilities-and-how-to-fix-them