TRABAJO DE FUNDAMENTOS DE COMPUTADORES Y REDES

Curso 2020-2021

INTRODUCCIÓN

El mundo te necesita. Ejércitos de gentes sin escrúpulos se dedican a atacar sistemas informáticos de manera continua y hacen falta expertos en seguridad con una buena base de los Fundamentos de Computadores y Redes. En esta asignatura hemos formado una fuerza de choque llamada FCR Hacking Force y tú formas parte de ella.

¿Qué vas a conseguir con el trabajo?

- Aplicar los conocimientos de la asignatura en un entorno realista, aunque simplificado. Verás cómo estos conocimientos son fundamentales para la seguridad informática.
- Entrar en contacto con una arquitectura real: la arquitectura Intel x86-32. Además, al conocer una segunda arquitectura en la asignatura, podrás comprobar cómo conceptos generales se pueden aplicar de distintas maneras en implementaciones concretas.
- Practicar el lenguaje C/C++, que es necesario para otras partes de la asignatura y para asignaturas futuras, además de ser un lenguaje muy usado en la práctica. Asimismo, verás cómo mezclarlo con ensamblador.
- Practicar el uso de máscaras y desplazamientos, elementos muy habituales en el software de sistemas, seguridad, tratamiento de imágenes o comunicaciones.
- Desarrollar habilidades de trabajo en grupo y documentación básicas para un Ingeniero en Informática.

DESARROLLO DEL TRABAJO

El trabajo se desarrollará en dos fases.

FASE 1 – CAMPO DE ENTRENAMIENTO (5 PUNTOS)

En esta fase vas a realizar una serie de ejercicios que servirán de entrenamiento para la fase 2, cuando tus habilidades se pondrán a prueba para proteger al mundo de un ataque.

Fase 1.1 – Ceremonia de iniciación (2,5 puntos)

Durante esta primera parte, tu grupo debe realizar un programa en C/C++ para practicar conceptos como manejo de máscaras, desplazamientos y cadenas. Para realizar este programa, debéis partir de la solución **Teamwork** que podéis descargar de la web de la FCR Hacking Force, http://merak.atc.uniovi.es/teamwork, donde debes entrar con tus credenciales de UniOvi.

El programa a desarrollar simula un control de acceso. Cada grupo tiene unas restricciones distintas. Las instrucciones para el tuyo estarán disponibles en la web de FCR Hacking Force pero sólo después de que el profesor haya creado el grupo.

Fase 1.2 – Supervivencia en código máquina (2,5 puntos)

A partir de la solución de Visual Studio presentada por tu grupo, debéis responder a una serie de cuestiones. Para cada una de ellas **debéis explicar los pasos que habéis seguido para hallar la solución, incluyendo las capturas de pantalla en las que se pueda comprobar de dónde se ha obtenido la respuesta.**

Se pide:

- (1 punto) Dirección de memoria a partir de la cual se sitúa el código de paso de parámetros a la función **IsValidAssembly()**. También debéis indicar cuál es ese código de paso de parámetros en forma de código máquina y mnemónicos.
- (0,5 puntos) Dirección de la memoria en la que se encuentra la primera cadena que se lee en la primera función indicada en las instrucciones.
- (0,5 puntos) Dirección de la memoria en la que se sitúa el epílogo de la primera función indicada en las instrucciones y el propio código del epílogo, en forma de código máquina y de mnemónicos.
- (0,5 puntos) Código máquina de la primera instrucción de ensamblador introducida en el ensamblador en línea de la cuarta función indicada en las instrucciones.

Vuestro grupo de trabajo tendrá un foro en el Campus Virtual y en él debéis realizar las entregas. El **viernes 19 de marzo** como muy tarde, debéis entregar un archivo comprimido en formato zip con el archivo de código fuente **.cpp,** el código fuente .**asm** y una memoria en PDF con el nombre del equipo, vuestros nombres y UO, un ejemplo de entrada válida y otro de una entrada inválida para cada función y la respuesta a las preguntas, con explicaciones y capturas de pantalla. Además, debéis indicar al final de la memoria cómo os habéis repartido el trabajo y cuántas horas ha dedicado cada uno.

FASE 2 – SALVANDO AL MUNDO (5 PUNTOS)

Ha llegado el momento de la verdad. El mundo está bajo una amenaza: unos criminales informáticos han situado una serie de bombas en infraestructuras críticas que sólo pueden ser desactivadas mediante unos programas llamados “bombas binarias”. Estos programas tienen 3 etapas. En cada una piden una entrada. Si cumple ciertos criterios, la etapa se desactiva y se pasa a la siguiente; si no, la bomba estalla. Si se consiguen desactivar todas las etapas, la bomba será desactivada. Vamos a trabajar todos juntos para lograrlo.

Por fortuna, una heroica incursión en los servidores de los atacantes nos ha permitido obtener el código fuente del programa principal de cada bomba y su información de depuración. En la web de FCR Hacking Force podrás obtener la bomba binaria que vuestro equipo tiene que desactivar. Para ello debéis deducir, a partir de la depuración del código, valores de entrada válidos.

Hemos descubierto, además, que las bombas binarias se conectan a un servidor C&C (Command and Control). En el mensaje de respuesta a la primera conexión se envía una cadena que identifica el subgrupo criminal que la ha preparado. Creemos que esta información puede ayudarnos a encontrarlos, así que debes obtenerla utilizando un analizador de red.

Estudiando el código, hemos visto que cuando se va avanzando por el código se mandan mensajes al servidor C&C. Además, cuando se desactivan todas las etapas se llama a la función **BombDisabled()** para informar de que se ha conseguido desactivar la bomba. Nos hemos hecho con el control de la IP del servidor C&C y se ha integrado en la web de la FCR Hacking Force, con lo que podrás ver hasta qué etapa ha conseguido desactivar en algún momento tu equipo.

La dirección de la FCR Hacking Force ha decidido que queremos conseguir modificar el código de cada bomba para que el servidor C&C crea que se ha deshabilitado sin necesidad de conocer las entradas válidas. Para ello, debéis encontrar una forma de modificar el código que logre este objetivo.

Los 5 puntos de esta fase se repartirán de la siguiente manera:

- Un punto por cada etapa que consigáis desactivar.
- Un punto por encontrar el nombre del subgrupo general que ha generado la bomba.
- Un punto por lograr modificar el código de la bomba para que indique que está desactivada sin introducir ninguna entrada válida.

En el foro para vuestro equipo del **Campus Virtual** se debe entregar, **viernes 7 de mayo** como muy tarde, un archivo .zip con el fichero .exe modificado para que se desactive sin necesidad de proporcionar entradas válidas y una memoria en formato PDF indicando las entradas que desactivan cada etapa y el proceso que habéis seguido para obtenerlas. Se deben utilizar capturas de pantalla en las explicaciones. Asimismo, se deben utilizar capturas de pantalla para mostrar cómo habéis obtenido el nombre del subgrupo criminal. También se debe explicar cómo se ha logrado modificar el código para que se desactive sin necesidad de introducir ninguna entrada. Si las explicaciones no son correctas, suficientes o claras, la nota indicada más arriba para cada aparto se verá reducida.

Por último, se debe indicar cómo se ha repartido el trabajo entre los miembros del grupo y cuántas horas ha dedicado cada uno.

EVALUACIÓN

La evaluación se realizará en base a las puntuaciones señaladas en la sección de desarrollo del trabajo. El resultado total dependerá de la calidad del código y de la redacción y presentación de la memoria. Esta nota podrá ser ponderada por otro factor en función de la aportación de cada alumno al trabajo. Cada día de retraso en la entrega de cualquiera de las fases restará 2 puntos.

Si se detecta que se ha realizado el trabajo por medios ilícitos o ha sido realizado por otras personas, la nota en la **evaluación continua** para **todos los miembros** del grupo será de **cero**.

INDICACIONES PARA EL DESARROLLO DEL TRABAJO

Para el desarrollo de la fase 1 es imprescindible haber realizado la sesión 1 del bloque 0 de prácticas de la asignatura, donde se introduce el lenguaje de programación C/C++.

En el sitio web de la FCR Hacking Force encontrarás una sección de recursos que incluirá documentos y vídeos de formación para poder realizar el trabajo.