UNIVERSIDAD COMPLUTENSE MADRID

ntic master

TAREA EVALUABLE

Máster en Ciberseguridad

MÓDULO

Ingeniería inversa y exploiting

PROFESOR:

D. Pablo San Emeterio

Contenido

1 En qué consiste la tarea evaluable

El alumno deberá hacer varias tareas que sirvan para afianzar los conocimientos que se enseñan en este módulo.

DISCLAIMER: Todos los ejercicios deben hacerse en el laboratorio de máquinas virtuales. Vamos a trabajar en algunos ejercicios con malware real. Para evitar el riesgo de infectar un equipo personal o pérdida de información personal se debe utilizar en todo momento una máquina virtual para trabajar. La UCM no se hace cargo de las consecuencias que puedan derivarse de no seguir las medidas indicadas.

En el módulo de Reversing vamos a hacer 3 ejercicios de tipo crackme. Estos ejercicios son retos en los que se debe encontrar la contraseña que los resuelve. Para ello se debe analizar la función o funciones que evalúan la contraseña introducida por el usuario. Se consideran resueltos los ejercicios cuando el alumno indica la contraseña, un pantallazo de la función analizada en el desensamblador, junto con una breve explicación de la lógica de la función.

Para el ejercicio 4 de reversing, el alumno debe darse de alta en la plataforma Atenea y resolver todos los ejercicios que se encuentran en el grupo de tareas “Básica: ransomware”

En el 5 ejercicio, deben analizar el malware y encontrar la clave que descifra el ransomware y validar que es correcta. Se debe dar la contraseña, una breve descripción de cómo se encontró y demostrar que se ha validado que la contraseña encontrada funciona.

Para los ejercicios de exploiting se deben entregar una memoria de no más de 3 páginas por ejercicio, en la que se describen los pasos realizados (incluyendo capturas de pantallas) para resolverlos.

1.1 Laboratorio compuesto por

Exploiting:

- Máquinas virtuales proporcionadas por el profesor (XP y W2K8)
- Máquinas virtuales creadas por el alumno (Kali)

Malware:

- Máquinas virtuales creadas por el alumno (W10 y reutilizar Kali)

1.2 Reversing

Valor: 5.5 puntos

1. Crackme1 **1 punto**
2. Crackme2 **1 punto**
3. Crackme en .Net **1 punto**
4. Ejercicios Ransomware Atenea **1.5 puntos**
5. Malware Real en .NET **1 punto**

1.2 Exploiting

Valor: 4.5 puntos

1. Explotar XP con metasploit **0.5 punto**
2. Analizar 2008 con nmap y explotar con exploit adecuado de metasploit **1 punto**
3. Analizar con masscan todos los rangos de IP de España en búsqueda de máquinas con el puerto 445 abierto. Emplear máquina de digitalocean u otro cloud provider.(https://m.do.co/c/b4b63d4cdf87). De las máquinas encontradas con el puerto 445 abierto lanzar nmap para detectar si son vulnerables a ethernalblue. **1 punto**

https://www.nirsoft.net/countryip/es.html

4. Realizar exploit de carpeta test1 (guaido en el manual) **1 punto**
5. Realizar exploit carpeta test2 y sustituir payload de calculadora por el payload de Shell_bind de meterpreter **1 punto**

2 Cómo entregar la tarea

El alumno debe subir su trabajo en un archivo ZIP con el siguiente patrón en el nombre del archivo:

TAREA_DNI_NOMBRE_APELLIDO1_APELLIDO2.zip

Cualquier duda o incidencia con la entrega se puede consultar directamente con el profesor a través del foro y chat del Campus de la Universidad.