Contents

1 Cuestionario

Pregunta 1
¿Qué significa que un pentesting sea de Caja Blanca?

Pregunta 2
Crea un diagrama explicando como funciana el bloque de RAM de una computador. Donde está el kernel, stack, el heap, etc.

Pregunta 3
Menciona el significado de los siguientes registro:

- EAX
- EBX
- EXC
- EDX
- ESI
- EDI
- EBP
- ESP
- EIP

Pregunta 4
¿Qué es little endian y big endian?¿Cuál usa tu procesador?

Pregunta 5
¿Qué es un segmento y que es un offset?

Pregunta 6
¿Que arquitectura tiene tu computadora?

Pregunta 7
¿Crées que esta vulnerabilidad desapareció con las nuevas funciones seguras como fgets?

2 Reporte

2.1 Recopilación

Pregunta
En esta fase analizarás tus herramientas, el código y todo lo que cuentas para llevar a cabo la práctica.

2.2 Análisis

Pregunta
Identificarás las vulnerabilidades y como aprovecharlas. Documentaras todo lo que llegues a encontrar.

2.3 Explotación

Pregunta
En esta etapa documentarás la creación de tu exploit, como llegaste al puntero base, y como usaste las herramientas para lograrlo.

2.4 Post-explotación

Pregunta
En esta fase explicarás tu exploit resultante, también las conclusiones a las cuales llegaste. Explicarás como corregir el código de la práctica y anexarás la correción en su respectiva carpeta.

2.5 Imagina

Pregunta
En esta fase intenta imaginar todo lo que podrias hacer utilizando esta vulnerabilidad. Explicalo detalladamente y reflexiona el alcance de esta vulnerabilidad.

References

[1] A

[2] B