

≡ 🔎 (https://profile.intra.42.fr/searches)

rnavarre

(https://profile.intra.42.fr)

SCALE FOR PROJECT TSUNAMI (/PROJECTS/TSUNAMI)

You should evaluate 1 student in this team



Git repository

git@vogsphere-v2.42madrid.com:vogsphere/intra-uuid-cfa80017

Introduction

Por favor, respeta las siguientes indicaciones:

- Sé educado, cortés, respetuoso y constructivo durante el proceso de evaluación. El bienestar de la comunidad depende de ello.
- Identifica con la persona o grupo evaluado los posibles fallos del trabajo presentado. Tómate el tiempo de discutir y debatir los problemas que hayas identificado.
- Debes entender que no todo el mundo entiende los enunciados del mismo modo, lo que quiere decir que vuestra visión del proyecto o lo que éste pide pueden variar. Mantén siempre una mente abierta y evalúa de la forma más sincera posible. El buen funcionamiento de la pedagogía se fundamenta en una evaluación correcta.

Guidelines

- No evalúes más que lo que figura en el repositorio git clonado del estudiante o del grupo.
- Asegúrate de que el repositorio git es efectivamente el del estudiante o el del grupo, que se trata del proyecto correcto, y que se ha lanzado «git clone» sobre un repositorio vacío.
- Asegúrate escrupulosamente de que no se ha utilizado para engañar ningún alias y de que va a corregir la entrega oficial.
- Con el fin de evitar sorpresas, verifica con el evaluado los eventuales scripts usados para facilitar la evaluación.
- Si, como evaluador, no has realizado el proyecto que vas a evaluar, debes leer el enunciado completamente antes de empezar a evaluar.
- Utiliza los flags disponibles para señalar una entrega vacía, un programa que no funcione, un error de norma, un problema de trampas... En esas situaciones, la evaluación se dará por finalizada y la nota será

0, o -42 si ha habido trampas. Sin embargo, salvo en los casos de trampas, te animamos a continuar con el intercambio de opiniones sobre el trabajo entregado, incluso no terminado, para identificar los problemas que han llevado al fracaso y evitar repetirlos en el futuro.

- A lo largo de toda la evaluación, no se tolerará ningún segfault ni ninguna parada del programa (inesperada, prematura o incontrolada)

En esos casos, la nota final será 0. Utiliza el flag correspondiente.

No deberías tener que editar jamás ningún fichero, salvo el de configuración, si es que existe. En el caso en el que desees modificar un fichero, debes explicar explícitamente por qué necesita editarlo y ponerte de acuerdo con el estudiante evaluado antes de tocar cualquier cosa.

Attachments

subject.pdf (<https://cdn.intra.42.fr/pdf/pdf/62333/es.subject.pdf>)

Parte obligatoria

Aplicación vulnerable

La aplicación vulnerable cumple con los siguientes apartados:

- Hace uso de la función strcpy.
- Se ha compilado con parámetros sin protecciones específicas para exploit.
- Se desborda la pila y permite el control del EIP. Si hay un error, debes parar la evaluación.

Yes

No

Creación de shellcode

La creación del shellcode cumple con los siguientes apartados:

- Lanza la calculadora de Windows XP.
- Encuentra una dirección de retorno válida en ese momento.
- Se desborda la pila y permite el control del EIP. Si hay un error, debes parar la evaluación.

Yes

No

Exploit

Se ha realizado un exploit para la aplicación vulnerable que cumple con los siguientes apartados:

- El exploit se ejecuta sin errores y en caso de fallar lo notifica.
- El shellcode se ejecuta de manera correcta.
- Se controlan todas las excepciones. Si hay un error, debes parar la evaluación.

Yes No

Extras

Solo se mirará la parte extra si su parte obligatoria es impecable. Eso supone que tendrá que completar la parte obligatoria desde el principio hasta el final y que su gestión de errores debe ser perfecta, incluso frente a situaciones retorcidas. Si durante la evaluación no se han atribuido todos los puntos, no se contabilizará ningún punto en la parte extra.

Linux Vulnerable

¿Se ha creado el exploit en una sistema operativo Linux Vulnerable?

 Yes No

Lenguaje de programación

¿Se ha creado el exploit en otro lenguaje de programación?

 Yes No

Ratings

Don't forget to check the flag corresponding to the defense

 Ok ★ Outstanding project Empty work Invalid compilation Cheat Crash Leaks ⚡ Forbidden function

Conclusion

Leave a comment on this evaluation

Finish evaluation

Terms of use for video surveillance (<https://profile.intra.42.fr/legal/terms/1>)

Legal notices (<https://profile.intra.42.fr/legal/terms/3>)