Webinar Gratuito

Desbordamiento de Búfer

Alonso Eduardo Caballero Quezada

Instructor y Consultor en Hacking Ético, Forense Digital & GNU/Linux

Sitio Web: https://www.ReYDeS.com -:- e-mail: ReYDeS@gmail.com

Jueves 7 de Enero del 2021

Alonso Eduardo Caballero Quezada

EXIN Ethical Hacking Foundation Certificate, LPIC-1 Linux Administrator Certified, LPI Linux Essentials Certificate, IT Masters Certificate of Achievement en Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling, Digital Forensics, Cybersecurity Management Cyber Warfare and Terrorism, Enterprise Cyber Security Fundamentals, Phishing Countermeasures Pen Testing, Certificate Autopsy Basics and Hands On, ICSI Certified Network Security Specialist y OSEH.

Más de 18 años de experiencia como consultor e instructor independiente en las áreas de Hacking Ético y Forense Digital. Ha dictado cursos presenciales y virtuales en Ecuador, España, Bolivia y Perú, presentándose también constantemente en exposiciones enfocadas a Hacking Ético, Forense Digital, GNU/Linux.

Redes Sociales

https://www.linkedin.com/in/alonsocaballeroquezada/

https://twitter.com/Alonso_ReYDeS

https://www.youtube.com/c/AlonsoCaballero

https://www.facebook.com/alonsoreydes/

https://www.reydes.com

reydes@gmail.com

+51 949 304 030

Desbordamiento de Búfer

Una condición de desbordamiento de búfer existe cuando un programa intenta poner más datos en un búfer del cual puede tener, o cuando un programa intenta poner datos en una área de memoria pasado un búfer.

En este caso, un búfer es una sección secuencial de memoria asignada para contener cualquier cosa, desde una cadena de caracteres hasta un arreglo de enteros.

Escribir fuera de los limites de un bloque de memoria asignada puede corromper datos, hacer caer un programa, o causar la ejecución de código malicioso.

* https://owasp.org/www-community/vulnerabilities/Buffer_Overflow

Desbordamiento de Búfer (Cont.)

Los desbordamientos de búfer no son fáciles de descubrir, e incluso cuando lo son, generalmente son muy difíciles de explotar. Pero los atacantes pueden identificarlos en una gran diversidad de productos y componentes.

En una explotación clásica, un atacante envía datos hacia un programa, los cuales son almacenados en un búfer de pila de tamaño insuficiente.

El resultados es la información de la pila de llamadas es sobrescrita. Los datos ajustan el puntero de retorno, de tal manera cuando la función retorna, transfiere el control hacia el código malicioso contenido en los datos del atacante.

* https://owasp.org/www-community/vulnerabilities/Buffer_Overflow

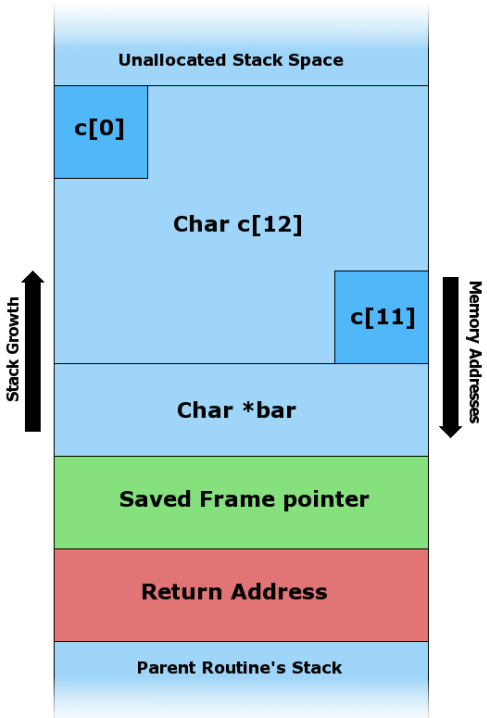
Explotar Desbordamiento de Búfer en Pila

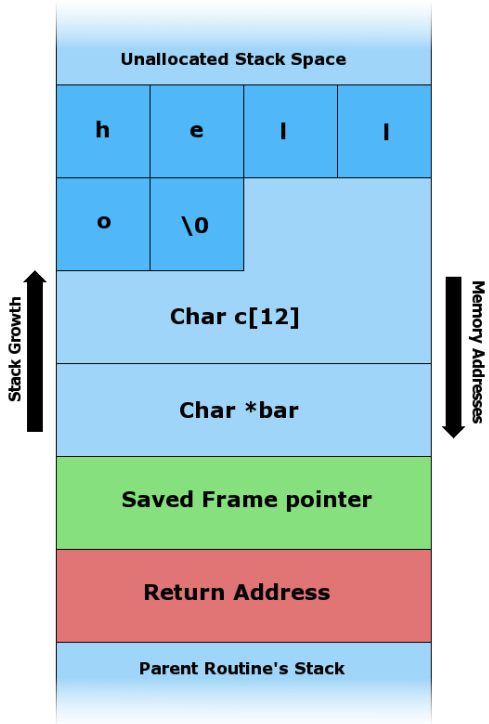
El método canónico para explotar un desbordamiento de búfer basado en pila , implica sobrescribir la dirección de retorno con un puntero hacia los datos controlados por el atacante.

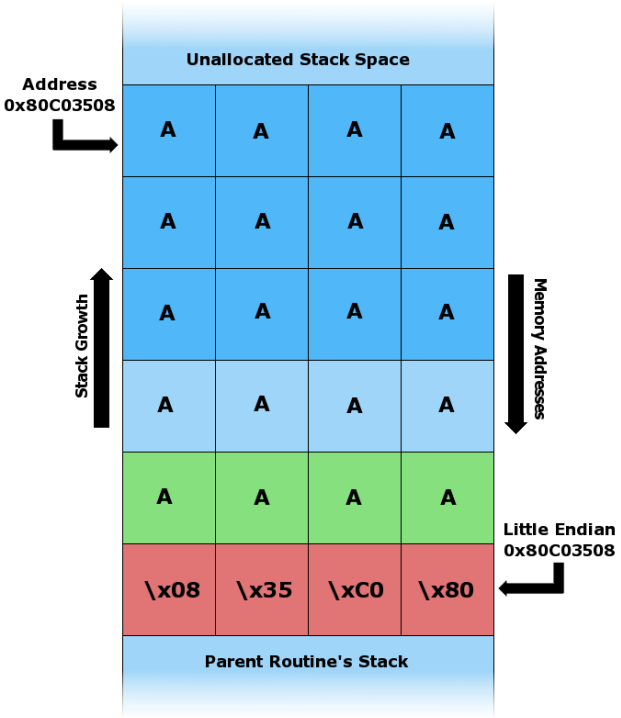
```c
#include <string.h>

void foo(char *bar)
{
   char c[12];

   strcpy(c, bar);  // no bounds checking
}

int main(int argc, char **argv)
{
   foo(argv[1]);
   return 0;
}
```

* https://en.wikipedia.org/wiki/Stack_buffer_overflow

Explotar Desbordamiento de Búfer en Pila







* https://en.wikipedia.org/wiki/Stack_buffer_overflow

GDB

El proyecto GNU para depuración de nombre GDB, permite ver aquello suscitándose dentro de otro programa mientras se ejecuta, o aquello lo cual estuvo suscitándose en el momento de su caída.

GDB puede hacer cuatro cosas principales (además de otras cosas en apoyo de estas) para ayudar a atrapar fallas en el acto:

- Iniciar un programa especificando algo lo cual podría afectar su comportamiento
- Hacer el programa se detenga sobre condiciones específicas
- Examinar aquello ocurrido cuando un programa se detuvo
- Cambiar cosas en el programa, de tal manera se puede experimentar corrigiendo los efectos de una falla, y continuar aprendiendo sobre otro

* GDB: https://www.gnu.org/software/gdb/

Curso

-

Curso Virtual Hacking Ético 2021

Domingos 10, 17, 24 y 31 de Enero 2021. De 9:00 am a 12:15 pm (UTC -05:00)

Este curso virtual ha sido dictado a participantes residentes en los siguientes países:

Presentación

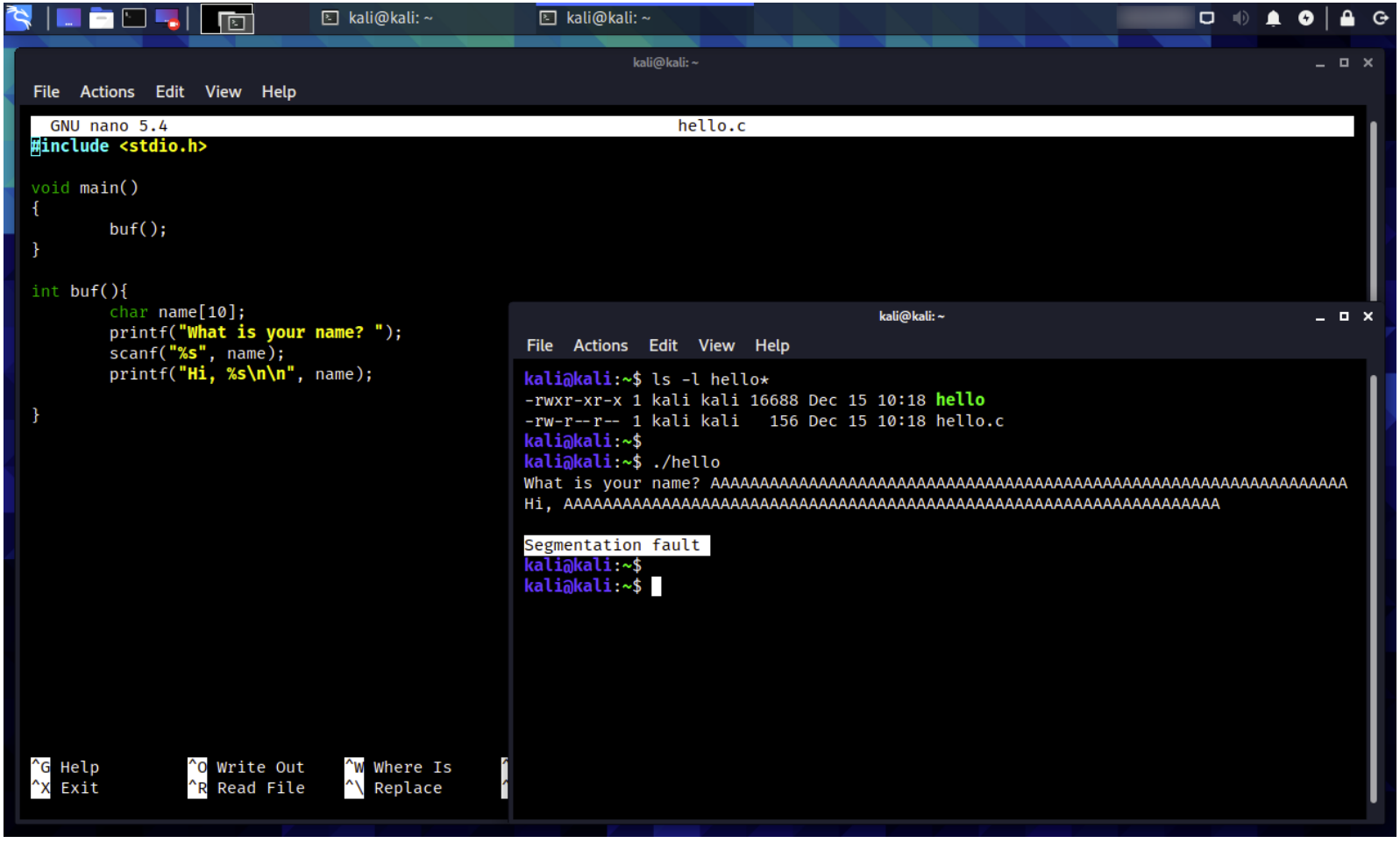
Como profesionales en ciberseguridad, se tiene la única responsabilidad de encontrar y entender las vulnerabilidades presentes en la organización, para luego trabajar diligentemente en mitigarlas antes de estas sean aprovechadas por los atacantes maliciosos. Este curso abarca las herramientas, técnicas y metodologías para realizar pruebas de penetración contra redes y sistemas, y así estar en la capacidad de realizar proyectos de pruebas de penetración exitosamente. Todas las organizaciones necesitan personal experimentado en seguridad de la información, quienes puedan encontrar vulnerabilidades y mitigar sus efectos. Con este curso se estará en la capacidad de realizar pruebas de penetración y hacking ético, aplicando los conocimientos, herramientas, y técnicas explicadas detalladamente. Consecuentemente descubrir y explotar vulnerabilidades en entornos reales, demostrando así todos los conocimientos adquiridos.

Alonso Eduardo Caballero Quezada es EXIN Ethical Hacking Foundation Certificate, LPIC-1 Linux Administrator, LPI Linux Essentials Certificate, IT Masters Certificate of Achievement en Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling, Digital Forensics, Cybersecurity Management, Cyber Warfare and Terrorism, Enterprise Cyber Security Fundamentals, Phishing Countermeasures, Pen Testing, Basic Technology Certificate Autopsy Basics and Hands On, ICSI Certified Network Security Specialist (CNSS) y OPEN-SEC Ethical Hacker (OSEH). Ha sido instructor en el OWASP LATAM Tour, expositor en OWASP Perú Chapter Meeting y OWASP LATAM at Home , además de Conferencista

Más Información: https://www.reydes.com/d/?q=Curso_de_Hacking_Etico

e-mail: reydes@gmail.com Sitio Web: https://www.reydes.com

Demostraciones

- 

Cursos Virtuales Disponibles en Video

Curso Virtual de Hacking Ético
https://www.reydes.com/d/?q=Curso_de_Hacking_Etico

Curso Virtual de Hacking Aplicaciones Web
https://www.reydes.com/d/?q=Curso_de_Hacking_Aplicaciones_Web

Curso Virtual de Informática Forense
https://www.reydes.com/d/?q=Curso_de_Informatica_Forense

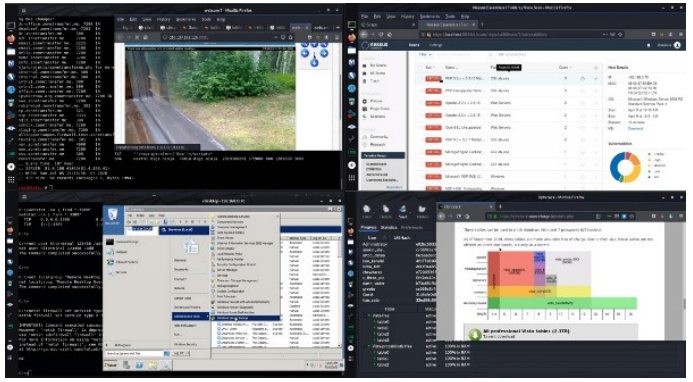
Curso Virtual Hacking con Kali Linux
https://www.reydes.com/d/?q=Curso_de_Hacking_con_Kali_Linux

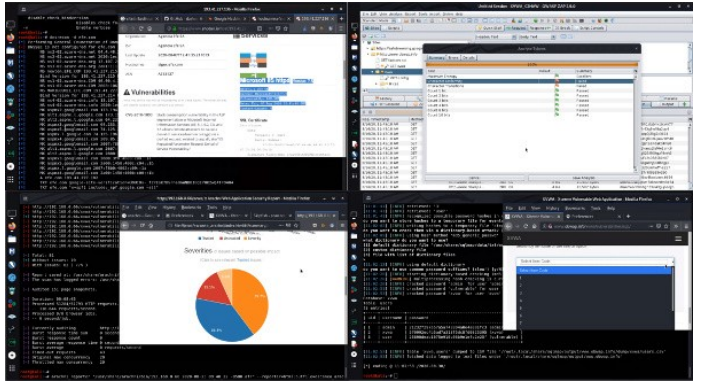
Curso Virtual OSINT - Open Source Intelligence
https://www.reydes.com/d/?q=Curso_de_OSINT

Curso Virtual Forense de Redes
https://www.reydes.com/d/?q=Curso_Forense_de_Redes

Y todos los cursos virtuales:

https://www.reydes.com/d/?q=cursos





Más Contenidos

Videos de 62 webinars gratuitos

https://www.reydes.com/d/?q=videos

Diapositivas de los webinars gratuitos

https://www.reydes.com/d/?q=eventos

Artículos y documentos publicados

https://www.reydes.com/d/?q=documentos

Blog sobre temas de mi interés

https://www.reydes.com/d/?q=blog/1

Webinar Gratuito

Desbordamiento de Búfer

Alonso Eduardo Caballero Quezada

Instructor y Consultor en Hacking Ético, Forense Digital & GNU/Linux

Sitio Web: https://www.ReYDeS.com -:- e-mail: ReYDeS@gmail.com

Jueves 7 de Enero del 2021