INDICE DEL CURSO DE REVERSING Y EXPLOITING CON HERRAMIENTAS FREE  
por RICARDO NARVAJA

EJERCICIOS:

<https://drive.google.com/drive/folders/1y3k4BeES81jBXf-PgsPpfHYfYDmowx3I?usp=sharing>

# PARTE 1 - 18/10/2019

INSTALACIÓN DE LAS HERRAMIENTAS NECESARIAS.

INSTALAR IDA FREE

INSTALAR RADARE

INSTALAR GHIDRA

INSTALAR X64DBG

INSTALAR WINDBG

INSTALAR PYTHON

INSTALAR PYCHARM COMMUNITY

[**https://docs.google.com/document/d/1vbXBvfYuZQW-N6wxmuM6-bDOkV3lguNUU78vpZ7nsQk/edit?usp=sharing**](https://docs.google.com/document/d/1vbXBvfYuZQW-N6wxmuM6-bDOkV3lguNUU78vpZ7nsQk/edit?usp=sharing)

# PARTE 2 - 26/10/2019

DEBUGGING CON X64DBG

DEFINICIÓN DE BUG

DEFINICIÓN DE VULNERABILIDAD

DEFINICIÓN DE EXPLOIT

DEFINICIÓN DE BUFFER

DEFINICIÓN DE BUFFER OVERFLOW

DEFINICIÓN DE AMPERSAND

DEBUGGEANDO EL EJERCICIO STACK 1 en X64DBG

PROLOGO - EPILOGO en 32 BITS

NUESTRA DEFINICIÓN DE HORIZONTE

<https://drive.google.com/open?id=1sDSUnAmD-yuS98-md6wV5G7pqCrMCegtYYNoUcfCbQ8>

# PARTE 3 - 6/11/2019

REVERSING ESTÁTICO PRIMEROS PASOS.

DEFINICIÓN DE BINARY DIFFING

REVERSING ESTÁTICO DEL STACK 1 CON IDA FREE

REVERSING ESTÁTICO DEL STACK 1 CON RADARE

REVERSING ESTÁTICO DEL STACK 1 - RADARE - USANDO CUTTER

REVERSING ESTÁTICO DEL STACK 1 USANDO GHIDRA

INSTALAR DIA SDK

REVERSING ESTÁTICO DEL STACK 2 CON IDA FREE

REVERSING ESTÁTICO DEL STACK 2 CON RADARE

REVERSING ESTÁTICO DEL STACK 2 -RADARE - USANDO CUTTER

REVERSING ESTÁTICO DEL STACK 2 USANDO GHIDRA

<https://drive.google.com/open?id=1qmVT3tpPmBjAvlOqUrTDFhrVfWD2rNnYnsHzcWQAxRc>

# PARTE 4 - 15/11/2019

DEFINIENDO CONCEPTOS NECESARIOS PARA LA SOLUCIÓN DE EJERCICIOS STACK 3 y 4.

DEFINICION DE CARACTER INVALIDO O BAD CHAR

SCRIPT BÁSICO PARA TESTEAR BAD CHARS

ADAPTANDO EL SCRIPT BASICO PARA PROBAR BAD CHARS EN STACK 1

SOLUCIÓN DEL STACK 3

PROPUESTAS PARA SOLUCIONAR EL STACK 4

<https://docs.google.com/document/d/1H9bMwcuGOtWrrJ9-RnLvCZURDURIb3q1Xefy0p81s2E/edit?usp=sharing>

# PARTE 5 - 29/11/2019

SOLUCIONANDO EL STACK 4 en IDA FREE.

ANALIZANDO ESTÁTICAMENTE EL STACK 4 EN IDA FREE.

RESTRICCIÓN POR BAD CHARS o CARACTER INVALIDO.

REPRESENTACIÓN ESTÁTICA DEL STACK DE LA FUNCION MAIN.

SOLUCIÓN ACEPTABLE DEL STACK 4 CON CRASH.

SOLUCIÓN PROFESIONAL DEL STACK 4 SIN CRASH NI HARCODING.

<https://drive.google.com/open?id=1KwG11lOAvLS2voKgX7aWdm9cO-a0_nAqK6ZUITzmXyY>

# PARTE 6 - 19/12/2019

SOLUCIONANDO EL ABO1 con RADARE.

SOLUCIONANDO EL ABO 1

USANDO RABIN2

EJECUTABLES ÚTILES INCLUIDOS CON RADARE

RAHASH2

RAX2

RASM2

RADIFF2

DIFERENCIAS ENTRE DIRECCIONES VIRTUALES Y FILE OFFSET.

REVERSING ESTÁTICO

OBTENER LOS BUILDS MÁS RECIENTES DE RADARE.

MAPA ESTÁTICO DEL STACK

DEBUGGEANDO

SHELLCODE CON RESOLVER.

RESOLVER DE 32 BITS.

EJECUTABLE STANDALONE CON SHELLCODE

USANDO WINDBG

Thread Environment Block (TEB)

Process Environment Block (PEB)

IMAGE\_DOS\_HEADER

IMAGE\_NT\_HEADERS

IMAGE\_OPTIONAL\_HEADERS

IMAGE\_DATA\_DIRECTORY\_ARRAY

IMAGE\_EXPORT\_DIRECTORY

<https://drive.google.com/open?id=1YKeXzD884crCiusxtPcHYLxwg2RRDNlLUYTdlC2HJs8>

# PARTE 7 - 24/01/2020

SOLUCIONANDO EL ABO2 con GHIDRA.

INSTALANDO GHIDRA 9.1.1

EXPLOTANDO SEH EN 32 BITS.

TIB y TEB

EXCEPTION REGISTRATION RECORDS

POP POP RET

SCRIPT Get-PESecurity

<https://docs.google.com/document/d/19v_lryoG6obl4KxNJtgBZGi1wNFbHRHobtMNsviKfes/edit?usp=drivesdk>

# PARTE 8 - 31/01/2020

SOLUCIONANDO EL ABO3 con IDA FREE.

MS DIA SDK ERROR

INSTALANDO VISUAL C++ 2008 REDISTRIBUTABLE

CÓDIGO FUENTE

ANÁLISIS ESTÁTICO DEL ABO3

SCRIPT SOLUCION

<https://drive.google.com/open?id=1lie9QK-woh5faHslypaIFeZA5SNqkrL5YcyoJwGpMzM>

# PARTE 9 - 07/02/2020

SOLUCIONANDO EL ABO4 con RADARE.

ACTUALIZANDO RADARE Y CUTTER

REVERSING DEL ABO4 USANDO RADARE

DEBUGGEANDO CON x64DBG

REVERSING DEL ABO4 USANDO CUTTER

<https://docs.google.com/document/d/1HHRtol9uvS1BT57To8LfgjHefyFRwRWBhvflUvDfLk8/edit?usp=drivesdk>

# PARTE 10 - 06/03/2020

Qué son las mitigaciones?

Que es DEP?

Que es Wow64?

Que es SetDEPProcessPolicy ?

Usando PROCESS EXPLORER

Que es ROP?

Qué son los GADGETS?

Reverseemos el ejecutable de 32 bits con DEP en GHIDRA.

SCRIPT SI EL PROGRAMA NO TUVIERA DEP

MINIROP DE PRACTICA.

USANDO RP++

<https://docs.google.com/document/d/1K5xebCWnZF1q66-H2hWABXdA94TF-mWygXyuU3aKvgM/edit?usp=drivesdk>

# PARTE 11 - 15/03/2020

ROPEANDO PASO A PASO

QUE ES ASLR?

PREGUNTAS:

1)Tiene módulos que no tengan ASLR?

2)Tiene en algun modulo que no tenga ASLR importada la funcion VIrtualAlloc o VirtualProtect?

3)Están los datos ya ubicados en el stack para comenzar a ropear?

4)Puedo pasar cualquier caracter o sea no hay caracteres inválidos?

Veamos la funcion VirtualAlloc en MSDN.

ROPEANDO SIN FINAL FELIZ

ROPEANDO CON FINAL FELIZ

VENCIENDO AL DEP

<https://docs.google.com/document/d/1z6BVZiiiXI5kwfqEqf0O4F3BUXcXCoLbITwwyFICVL8/edit?usp=drivesdk>

# PARTE 12 - 21/03/2020

COMENZANDO CON 64 BITS

CALLING CONVENTIONS EN 32 BITS.

ORDEN INVERSO o REVERSE ORDER

CALLING CONVENTION \_\_CDECL

CALLING CONVENTION \_\_STDCALL

CALLING CONVENTIONS EN 64 BITS.

MICROSOFT x64 CALLING CONVENTION

REGISTROS EN 64 BITS

REVERSEANDO EN 64 BITS

RESOLUCIÓN DEL EJERCICIO DE 64 BITS :Primera parte del ROP

<https://docs.google.com/document/d/1rmBgQiNE6FWpwo8AXKElPD0wDB538lX2gd5hmU_l8UY/edit?usp=drivesdk>

# PARTE 13 - 23/03/2020

RESOLUCIÓN DEL EJERCICIO DE 64 BITS

SCRIPT CON SOLUCIÓN COMPLETA

RESOLVER 64 BITS

ESTRUCTURAS DE 64 BITS

HALLANDO LA IMAGEBASE DE KERNEL32

HALLANDO LA DIRECCIÓN DE WINEXEC

LLAMANDO A WINEXEC

<https://drive.google.com/open?id=1UTIQe5vnIHg2gaUNs_9OJ_92UZ4Do5uLTgda42k19VM>

# PARTE 14 - 18/04/2020

ANALIZANDO LA DIFICULTAD DEL SEGUNDO EJERCICIO DE 32 BITS

CONTESTANDO LAS PREGUNTAS

1)Tiene módulos que no tengan ASLR?

2)Tiene en algun modulo que no tenga ASLR importada la funcion VIrtualAlloc o VirtualProtect?

3)Están los datos ya ubicados en el stack para comenzar a ropear?

4)Puedo pasar cualquier caracter o sea no hay caracteres inválidos?

SCORE FINAL

TIP PARA AYUDAR A QUE LO INTENTEN RESOLVER

<https://docs.google.com/document/d/1PfK2jqr-i_kUEjp1f5J49CYoq9YDALi1mHM2orNdRJQ/edit#>

# Part 15 - 26/04/2020

EJERCICIO DE REVERSING 2 - 32 BITS CON RADARE

ABRIENDO PROYECTO GUARDADO (PO)

RENOMBRANDO FUNCIONES (AFN)

DUDAS SOBRE UN COMANDO (?)

NAVEGANDO MENUS (M)

WINDOW MODE(w)

BUSCANDO

ENCONTRANDO REFERENCIAS

BUSCANDO GADGETS.

REVERSEANDO ESTATICAMENTE.

HOUSTON TENGO UN PROBLEMA.

SCRIPT BASICO PARA EMPEZAR A ROPEAR.

<https://docs.google.com/document/d/1AMeeqyQ9IkrZFcRz5E4JbcOZ1QdhWVR1-NtiQU6m-2c/edit#>

# Part 16 - 04/05/2020

BUSCANDO GADGET CON RADARE

PROBANDO RADARE DEBUGGER

HOUSTON TENEMOS UN PROBLEMA.

SUFRIENDO BASTANTE.

EJECUTANDO UN SHELLCODE DIFERENTE

SCRIPT SOLUCIÓN FINAL PARA PYTHON 3.

<https://docs.google.com/document/d/1tutGlLjZTDtFGYqFqcczOKPiDmk-anvOqFxft3f2jiw/edit#heading=h.2okuuhjrhrfu>

# 

# Part 17 - 23/05/2020

REVERSEANDO EL EJERCICIO DE 64 BITS con GHIDRA

DECOMPILANDO CON GHIDRA

ROPEANDO EN 64 BITS

TRUCOS MICROSOFTIANOS

NOTA para MICROSOFT

MÁS TRUQUITOS MARCA MICROSOFT NO FUNCIONA WINEXEC

FUNCIONANDO A PESAR DE TODO

<https://drive.google.com/open?id=1_J8G08nv9x_Ht_Dmz7HLAzMNix5C6gmC2TuKLcxh5xg>

# Part 18 - 02/06/2020

IDC SCRIPTING

SCRIPT PARA BUSCAR GADGETS

SCRIPT FINAL

<https://t.co/K1BXZbHreb?amp=1>

# Part 19 - 22/08/2020

MANEJO DE ESTRUCTURAS CON SIMBOLOS

EJERCICIO SIN\_ESTRUCTURAS EN IDA FREE

EJERCICIO CON\_ESTRUCTURAS EN IDA FREE

PREPARANDO EL EJERCICIO CON\_ESTRUCTURAS EN IDA FREE SIN SÍMBOLOS.

<https://docs.google.com/document/d/13jU_bohMfYNK1T2lCF7gbtNVcGRFSgEpL4z2dNdm930/edit?usp=sharing>

# Part 20 - 25/09/2020

MANEJO DE ESTRUCTURAS SIN SÍMBOLOS

EJERCICIO CON\_ESTRUCTURAS EN IDA FREE SIN SÍMBOLOS

CREANDO UNA ESTRUCTURA VACÍA PARA REVERSEAR

REVERSING ESTÁTICO

EJECUTANDO EL NOTEPAD.

<https://docs.google.com/document/d/11ks_ncrpPV1vt8dLQ8kfjVgKeyuN1z2THmso-BYVrmI/edit?usp=sharing>

# Part 21 - 04/11/2020

MANEJO DE ESTRUCTURAS EN RADARE CON SÍMBOLOS

EJERCICIO CON ESTRUCTURAS EN RADARE CON SÍMBOLOS

RADARE MODO VISUAL SIN PANELS

ASIGNANDO ESTRUCTURAS

BUG EN ARRAYS DENTRO DE ESTRUCTURAS.

COLOCANDO COMENTARIOS

TERMINANDO USANDO COMENTARIOS HASTA QUE SE ARREGLE EL BUG

<https://docs.google.com/document/d/1ii8DgLgTc2JgtMKLuDNqTZOiNK4kOKnH1Z8ifj8Mx6c/edit?usp=sharing>