INDICE DEL CURSO DE REVERSING CON IDA DESDE CERO

<https://drive.google.com/open?id=1ylHQl3gaT1QT_-lbPsczEtRi-otdNPVd>

# INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO.

Contents

[INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO. 1](#_Toc40942588)

[PORQUE IDA PRO? 1](#_Toc40942589)

[LO PRIMERO ES LO PRIMERO 3](#_Toc40942590)

<https://drive.google.com/open?id=1iHVyacPkYAihYa184-I5EyAIn1ZK_mDP>

# INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 2.

Contents

[INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 2. 1](#_Toc40943616)

[SISTEMA NUMERICO 1](#_Toc40943617)

[NUMEROS NEGATIVOS en HEXADECIMAL 3](#_Toc40943618)

[POSITIVOS 6](#_Toc40943619)

[NEGATIVOS 6](#_Toc40943620)

[CARACTERES ASCII 6](#_Toc40943621)

[POSIBILIDADES DE BUSQUEDA 9](#_Toc40943622)

[NEXT CODE 9](#_Toc40943623)

[NEXT DATA 10](#_Toc40943624)

[SEARCH EXPLORED Y UNEXPLORED 11](#_Toc40943625)

[SEARCH INMEDIATE VALUE - SEARCH NEXT INMEDIATE VALUE 12](#_Toc40943626)

[SEARCH TEXT –SEARCH NEXT TEXT 12](#_Toc40943627)

[SEARCH SEQUENCE OF BYTES 14](#_Toc40943628)

[SEARCH NOT FUNCTION 15](#_Toc40943629)

<https://drive.google.com/open?id=1BF3PCXApFkNFUSCl9zBNBONaPQ3dwi3->

# INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 3

Contents

[INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 3 1](#_Toc40944078)

[EL LOADER 1](#_Toc40944079)

[Ahora para que sirven y que son exactamente los registros? 1](#_Toc40944080)

[Registros de propósito múltiples 2](#_Toc40944081)

[INSTRUCCIONES 4](#_Toc40944082)

[Instrucciones de Transferencia de Datos 5](#_Toc40944083)

<https://drive.google.com/open?id=1pxhB59YTuEz0lYxfCpb7TP_2TON8iYzJ>

# INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 4

Contents

[INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 4 1](#_Toc40944322)

[Mas instrucciones de transferencia de datos en IDA. 1](#_Toc40944323)

[KEYPATCH 7](#_Toc40944324)

[INSTRUCCIONES ESPECIFICAS DE TRANSFERENCIA RELATIVAS AL STACK O PILA 9](#_Toc40944325)

[QUE ES EL STACK o PILA? 9](#_Toc40944326)

<https://drive.google.com/open?id=1-j8F97YGEHO2Y2lS8amw314-PG4eCMT4>

# INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 5

Contents

[INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 5 1](#_Toc40945781)

[Mas instrucciones 1](#_Toc40945782)

<https://drive.google.com/open?id=1EBvg0uPsKw6tcy-4fdANTLNa-fXSzRLH>

# INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 6.

Contents

[INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 6. 1](file:///C:\Users\ricnar\Desktop\IDA%20DESDE%20CERO\ricardonarvaja.info(2)\6-INTRODUCCION%20AL%20REVERSING%20CON%20IDA%20PRO%20DESDE%20CERO%20PARTE%206\6-INTRODUCCION%20AL%20REVERSING%20CON%20IDA%20PRO%20DESDE%20CERO%20PARTE%206\6-INTRODUCCION%20AL%20REVERSING%20CON%20IDA%20PRO%20DESDE%20CERO%20PARTE%206.docx#_Toc40945674)

[Instrucciones aritméticas y lógicas. 1](file:///C:\Users\ricnar\Desktop\IDA%20DESDE%20CERO\ricardonarvaja.info(2)\6-INTRODUCCION%20AL%20REVERSING%20CON%20IDA%20PRO%20DESDE%20CERO%20PARTE%206\6-INTRODUCCION%20AL%20REVERSING%20CON%20IDA%20PRO%20DESDE%20CERO%20PARTE%206\6-INTRODUCCION%20AL%20REVERSING%20CON%20IDA%20PRO%20DESDE%20CERO%20PARTE%206.docx#_Toc40945675)

<https://drive.google.com/open?id=1CGI0LbyEDUp3iJjaXkCrl2DOoKNFw7fW>

# INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 7

Contents

[INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 7 1](#_Toc40946526)

[INSTRUCIONES DE CONTROL DE FLUJO 1](#_Toc40946527)

[SALTOS CONDICIONALES 7](#_Toc40946528)

[CALL Y RET 8](#_Toc40946529)

<https://drive.google.com/open?id=1E328ZXawEOls2iZ5IoFh44cFVJBfdL-D>

# INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 8.

Contents

[INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 8. 1](#_Toc40946642)

[EL LOADER 1](#_Toc40946643)

<https://drive.google.com/open?id=1SkI9wi1N-TONAA_73BhWs58mAduvnO6d>

# INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 9.

Contents

[INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 9. 1](#_Toc40946821)

[PRACTICA CON CRACKME HOLA\_REVERSER. 1](#_Toc40946822)

[¿Como podemos saber en IDA el largo de un buffer del stack si no tenemos el código fuente? 6](#_Toc40946823)

<https://drive.google.com/open?id=10X4tPV1H6RIgRcBy3ZfxaV8m9ofCcLvD>

# INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 10

Contents

[INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 10 1](#_Toc40947038)

[LOADER Y DEBUGGER 1](#_Toc40947039)

[¿Como sabemos si en una operación se considera el signo o no? 14](#_Toc40947040)

<https://drive.google.com/open?id=1c8_KbzW6FlsRMY1jyDur35qB0SsRaM27>

# INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 11.

Contents

[INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 11. 1](#_Toc40947895)

[BUG EN VERSION 6.8 1](#_Toc40947896)

[FLAGS 3](#_Toc40947897)

[CARRY FLAG 3](#_Toc40947898)

[OVERFLOW FLAG 6](#_Toc40947899)

[FLAG DE SIGNO 7](#_Toc40947900)

[ZERO FLAG 8](#_Toc40947901)

<https://drive.google.com/open?id=1fhPsbR0YSEnQ6y-HpAaGG8JgiG1SxdAx>

# INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 12.

Contents

[INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 12. 1](#_Toc40948067)

[PRACTICA TEST\_REVERSER. 1](#_Toc40948068)

[MOVSX Y MOVZX 15](#_Toc40948069)

[¿Y que hace la función CHECK con ambos? 20](#_Toc40948070)

<https://drive.google.com/open?id=19zqXbXysJJT7uWwJ7HHYZFxWzAWJ_q7f>

# INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 13

Contents

[INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 13 1](#_Toc40948526)

[PLUGINS INTERESANTES 1](#_Toc40948527)

[IPYIDA 1](#_Toc40948528)

[IPYTHON 2](#_Toc40948529)

[PROBLEMAS AL INSTALAR 14](#_Toc40948530)

<https://drive.google.com/open?id=17iT_5_WsofRzUBt4haWZc3c1DzNsOo5U>

# INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 14.

Contents

[INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 14. 1](#_Toc40948734)

[Desempacaremos el archivo CRACKME.exe empacado con UPX. 1](#_Toc40948735)

[Archivos empacados 1](#_Toc40948736)

[ORIGINAL 3](#_Toc40948737)

[PACKEADO 3](#_Toc40948738)

<https://drive.google.com/open?id=1EQn38QrbZdG_bvDyz9CqsxRHNqkC6Hll>

# INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 15.

Contents

[INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 15. 1](#_Toc40949059)

[DUMPEADO y la RECONSTRUCCION DE LA IAT. 1](#_Toc40949060)

[¿QUE ES LA IAT? 5](#_Toc40949061)

[¿Y cuál es el problema sino reconstruimos la IAT? 11](#_Toc40949062)

[SCYLLA. 11](#_Toc40949063)

<https://drive.google.com/open?id=1PVajINqPuTufNshdyYugKUbpotPY0Yqh>

# 

# INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 16.

Contents

[INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 16. 1](#_Toc40949209)

[DESEMPACANDO UnPackMe\_ASPack 2.2. 1](#_Toc40949210)

[PEEDITOR. 9](#_Toc40949211)

<https://drive.google.com/open?id=1yCuDbNMgqBQGUF-sDiiKDFNQe50dOdOw>

# INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 17.

Contents

[INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 17. 1](#_Toc40949539)

[RESOLVIENDO EL EJERCICIO PENDIENTE. 1](#_Toc40949540)

[DESEMPACANDO REMOTO. 1](#_Toc40949541)

[DLL CHARACTERISTICS Y RANDOMIZACION. 14](#_Toc40949542)

<https://drive.google.com/open?id=169S_ggSwNduxlPfaLgFYa_B3_tnu5BCr>

# INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 18.

Contents

[INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 18. 1](#_Toc40949799)

[REVERSEANDO EL DESEMPACADO. 1](#_Toc40949800)

[Representación estática del stack. 11](#_Toc40949801)

<https://drive.google.com/open?id=1mwZmhP29nM-NXqm662DbzZ9mQGwsRzDg>

# INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 19.

Contents

[INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 19. 1](#_Toc40949989)

[REVERSEANDO EL CRACKME DE CRUEHEAD. 1](#_Toc40949990)

[KEYGEN CRACKME DE CRUEHEAD. 15](#_Toc40949991)

<https://drive.google.com/open?id=1phm70OUNYAcXafhTJWf_WvrMxvoxSPoo>

# INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 20

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Contents

[INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 20 1](#_Toc40950344)

[Vulnerabilidades. 1](#_Toc40950345)

[Que es una vulnerabilidad? 1](#_Toc40950346)

[STACK OVERFLOW. 1](#_Toc40950347)

<https://drive.google.com/open?id=13sNvn_qgOrUEN6gSPlD4UuSQJ5t9AAV5>

# INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 21

Contents

[INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 21 1](#_Toc40950616)

[¿VULNERABLE O NO? 1](#_Toc40950617)

[BUFFER OVERFLOW. 4](#_Toc40950618)

<https://drive.google.com/open?id=1POiYBx9apJXyFM9j8SXKgpCyhjTA85OC>

# INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 22

Contents

[INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 22 1](#_Toc40950877)

[DIFFERS 1](#_Toc40950878)

[BINDIFF. 1](#_Toc40950879)

[TURBODIFF 10](#_Toc40950880)

[DIAPHORA 16](#_Toc40950881)

https://drive.google.com/open?id=1uhwHOzCnWTYMOTFNoIsxaPz4rqra3pyC

# 

# INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 23

Contents

[INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 23 1](#_Toc40951046)

[EJERCICIO IDA1.exe 1](#_Toc40951047)

<https://drive.google.com/open?id=1iWBN9Jnyh77r4I6VcPw4OFp9G7QkxAIa>

# 

# INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 24

Contents

[INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 24 1](#_Toc40951174)

[EJERCICIO IDA2.EXE 1](#_Toc40951175)

<https://drive.google.com/open?id=1_LZ1f0FqH0H5wE1JoZsPgCkSruMQUqO5>

# INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 25.

Contents

[INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 25. 1](#_Toc40951401)

[ESTRUCTURAS 1](#_Toc40951402)

[Que es una estructura? 1](#_Toc40951403)

[Soluciones del IDA3 y IDA4. 25](#_Toc40951404)

<https://drive.google.com/open?id=1wT6nRQHFkxggu-wn3n1CPVjEVnFGL9Ef>

# 

# INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 26

Contents

[INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 26 1](#_Toc40951612)

[MAS SOBRE ESTRUCTURAS. 1](#_Toc40951613)

<https://drive.google.com/open?id=1MdLWP9XVbqOD5c7h9firgLkXXS_8Ynuq>

# INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 27

Contents

[INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 27 1](#_Toc40952028)

[SOLUCIONANDO IDA\_STRUCT.7z. 1](#_Toc40952029)

[PROXIMITY VIEW 4](#_Toc40952030)

<https://drive.google.com/open?id=1Gn-k85Y6ZVqqHNGsq3OGZ2iurp8auhvN>

# INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 28

Contents

[INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 28 1](#_Toc40952458)

[UN POCO DE TEORIA. 1](#_Toc40952459)

[EJEMPLO1.exe 4](#_Toc40952460)

[EJEMPLO2.EXE 5](#_Toc40952461)

[PUNTEROS. 8](#_Toc40952462)

[PSEUDOCODIGO. 10](#_Toc40952463)

<https://drive.google.com/open?id=19VnRyY9clxpz-q6UGR28qsufSiDpNTo4>

# INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 29.

Contents

[INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 29. 1](#_Toc40952654)

[PROGRAMAS REALES Y CVE. 1](#_Toc40952655)

[PRACTICANDO DIFFEAR. 1](#_Toc40952656)

<https://drive.google.com/open?id=1gx2eCz2C8PydkWf7fZsHgKxPvxz9JfFI>

# INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 30.

Contents

[INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 30. 1](#_Toc40953152)

[VLC ( CVE-2008-4654) 1](#_Toc40953153)

[USANDO BINDIFF. 2](#_Toc40953154)

[USANDO TURBODIFF. 5](#_Toc40953155)

<https://drive.google.com/open?id=1A5k2qxW5Rtn8rfi5nkIHERHpKI_N8YuE>

# INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 31.

Contents

[INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 31. 1](#_Toc40953426)

[EXPLICACION DE LA SOLUCION DEL CVE. 1](#_Toc40953427)

<https://drive.google.com/open?id=1t6mOGqe45qdkTEPbG-C0Tmusz3zxkTT0>

# 

# INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 32.

Contents

[INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 32. 1](#_Toc40953686)

[WINDBG MAS IDA. 1](#_Toc40953687)

[Preparando Windbg para trabajar con IDA. 1](#_Toc40953688)

[COMANDOS DE WINDBG. 5](#_Toc40953689)

[CONFIGURANDO LOS SIMBOLOS PARA WINDBG. 7](#_Toc40953690)

<https://drive.google.com/open?id=1pzzsHrhtmVmd1lzdkMUjmc4h6UiAiV5B>

# INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 33.

Contents

[INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 33. 1](#_Toc40953905)

[PLUGINS PARA WINDBG STANDALONE. 1](#_Toc40953906)

[PYKD y MONA. 1](#_Toc40953907)

<https://drive.google.com/open?id=1dUfbP5zRqdDfxfVD7WQIFlRDPH2_iFSI>

# INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 34

Contents

[INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 34 1](#_Toc40954230)

[QUE ES DEP? 1](#_Toc40954231)

[SETDEPPROCESSPOLICY. 2](#_Toc40954232)

[ROP o return oriented programming. 5](#_Toc40954233)

<https://drive.google.com/open?id=1bz0hN-pYozWur6wexFqdjLT6K6vjn0Vw>

# INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 35

Contents

[INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 35 1](#_Toc40955856)

[DEP Y NO DEP. 1](#_Toc40955857)

[IDASPLOITER. 1](#_Toc40955858)

<https://drive.google.com/open?id=1lVFc2nbB80upduNV3xPeElCBovcJ57dn>

# 

# INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 36

Contents

[INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 36 1](#_Toc40956188)

[SOLUCIONANDO DEP.EXE 1](#_Toc40956189)

[¿Qué se puede hacer? 5](#_Toc40956190)

[USANDO GADGETS. 5](#_Toc40956191)

[VENCIMOS. 26](#_Toc40956192)

<https://drive.google.com/open?id=1_wCHAK32qypZhaRSveEzAzIC4h1lIQnm>

# INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 37

Contents

[INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 37 1](#_Toc40956378)

[USANDO MONA EN WINDBG. 1](#_Toc40956379)

[CARGANDO MONA 3](#_Toc40956380)

[ROP FINAL 14](#_Toc40956381)

<https://drive.google.com/open?id=10bMtFjvRVpPL0XbJek6cy8nar1_lDyaS>

# INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 38

Contents

[INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 38 1](#_Toc40956790)

[CANARY and SEH. 1](#_Toc40956791)

[CANARY\_sin\_DEP.exe 1](#_Toc40956792)

[\_EXCEPTION\_REGISTRATION\_RECORD 8](#_Toc40956793)

[SAFE SEH ON/OFF. 13](#_Toc40956794)

[NEXT Y SEH 23](#_Toc40956795)

<https://drive.google.com/open?id=1R4oDXr5YIHiBq0CGFKKL-Vya10jvNO12>

# INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 39

Contents

[INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 39 1](#_Toc40956993)

[CANARY\_con\_DEP.EXE 1](#_Toc40956994)

[AGAFI 5](#_Toc40956995)

<https://drive.google.com/open?id=1n2J5ofFXW5JpfGXRR4hLQnxscSVP7ee_>

# INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 40.

Contents

[INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 40. 1](#_Toc40957226)

[SHELLCODE UNIVERSAL 1](#_Toc40957227)

<https://drive.google.com/open?id=1XWtfJiQvMAU2Rk4QKAkYdVoROHfdcc-e>

# INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 41.

Contents

[INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 41. 1](#_Toc40957597)

[EJEMPLO STACK Y HEAP. 1](#_Toc40957598)

<https://drive.google.com/open?id=1P08-JS-HFjslZjSAzyhdfuajExUAabca>

# INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 42

Contents

[INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 42 1](#_Toc40957799)

[EJERCICIOS PENDIENTES. 1](#_Toc40957800)

<https://drive.google.com/open?id=1Mde2yiUFmFwkLEPkn4k5a2fAEO_y9He3>

# INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 43

Contents

[INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 43 1](#_Toc40958108)

[Solucionando la práctica 41b. 1](#_Toc40958109)

[CRASH OBTENIDO DE UN FUZZER. 16](#_Toc40958110)

[GFLAGS Y FULL PAGE HEAP. 20](#_Toc40958111)

<https://drive.google.com/open?id=13zgyrRoDQ2PX8uBUcr3jevmTPAAqpINg>

# INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 44.

Contents

[INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 44. 1](#_Toc40958312)

[MAS WINDBG DENTRO DE IDA VIENDO HEAP. 1](#_Toc40958313)

[HISTORIA DE LA ALLOCACION. 8](#_Toc40958314)

<https://drive.google.com/open?id=1nCDZP7LCs65b8CY27Fqo_aZk8sbskRS4>

# INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 45.

Contents

[INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 45. 1](#_Toc40958451)

[MONA EN PRACTICA41b. 1](#_Toc40958452)

<https://drive.google.com/open?id=1cb8UlFASXyCVElZLJ2DJP40Ykjme6nG2>

# INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 46.

Contents

[INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 46. 1](#_Toc40958755)

[EJERCICIO de la parte 44. 1](#_Toc40958756)

[MASAJEANDO EL HEAP. 12](#_Toc40958757)

<https://drive.google.com/open?id=1K4Cl2pPpOxVv9vvFu9zHi2zhV8VYQx35>

# INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 47.

Contents

[INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 47. 1](#_Toc40959236)

[EJERCICIO de la parte 44 1](#_Toc40959237)

[LOW FRAGMENTATION HEAP 3](#_Toc40959238)

[HEAP ESTANDAR Y LOW FRAGMENTATION HEAP WINDOWS 7. 4](#_Toc40959239)

<https://drive.google.com/open?id=18_72WpRXeCAb_4OL3s3GyErVC6_k2kDQ>

# INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 48

Contents

[INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 48 1](#_Toc40959936)

[ALLOCA EN LFH O HEAP ESTÁNDAR? 1](#_Toc40959937)

[RtlpAllocateHeap o RtlpLowFragHeapAllocFromContext 22](#_Toc40959938)

<https://drive.google.com/open?id=1QsmuEZuhncOQvwxYpPoDa4-LcMN3L48v>

# INTRODUCCION AL REVERSING CON IDA PRO DESDE CERO PARTE 49.

Contents

[INTRODUCCION AL REVERSING CON IDA PRO DESDE CERO PARTE 49. 1](#_Toc40960295)

[USE AFTER FREE 1](#_Toc40960296)

<https://drive.google.com/open?id=1Ct8jDEogklxmot-HghfE2mLmNxiGZ1EC>

# INTRODUCCION AL REVERSING CON IDA PRO DESDE CERO PARTE 50.

Contents

[INTRODUCCION AL REVERSING CON IDA PRO DESDE CERO PARTE 50. 1](#_Toc40961054)

[TRABAJANDO CON EL KERNEL DE WINDOWS. 1](#_Toc40961055)

[QUE ES EL KERNEL? 1](#_Toc40961056)

[ESPACIO DE DIRECCIONES VIRTUALES. 3](#_Toc40961057)

[VMWARE WORKSTATION 4](#_Toc40961058)

[CREANDO EL ENTORNO. 5](#_Toc40961059)

[SIMBOLOS 5](#_Toc40961060)

[OSR DRIVER LOADER 7](#_Toc40961061)

[Virtual KD 7](#_Toc40961062)

[CONTEXTOS 14](#_Toc40961063)

[SWITCHEANDO. 21](#_Toc40961064)

[RELOAD 22](#_Toc40961065)

[HELLOWORLDDRIVER 28](#_Toc40961066)

[USANDO IDA PARA DEBUGGEAR KERNEL. 37](#_Toc40961067)

<https://drive.google.com/open?id=17lBKtTK40uFUQkJeMfHACqR063SiR3UA>

# INTRODUCCION AL REVERSING CON IDA PRO DESDE CERO PARTE 51 KERNEL.

Contents

[INTRODUCCION AL REVERSING CON IDA PRO DESDE CERO PARTE 51 KERNEL. 1](#_Toc40961342)

[VIDEOTUTES. 1](#_Toc40961343)

[MAS DRIVER EN KERNEL 1](#_Toc40961344)

[DRIVER OBJECT 2](#_Toc40961345)

<https://drive.google.com/open?id=1LC9IAYyc-n6x2t80RYgg1vO9bzirwOYj>

# INTRODUCCION AL REVERSING CON IDA PRO DESDE CERO PARTE 52 KERNEL

Contents

[INTRODUCCION AL REVERSING CON IDA PRO DESDE CERO PARTE 52 KERNEL 1](#_Toc40961652)

[MAS KERNEL 1](#_Toc40961653)

[IOCTL 1](#_Toc40961654)

[DEVICE OBJECT 1](#_Toc40961655)

[Parameters 3](#_Toc40961656)

[\_DRIVER\_OBJECT 13](#_Toc40961657)

[SYMBOLIC LINK 15](#_Toc40961658)

[MajorFunction 17](#_Toc40961659)

[IRP 21](#_Toc40961660)

[DeviceIoControl 23](#_Toc40961661)

<https://drive.google.com/open?id=1ncCzkcVAR7yOR_tIlrWwQpQpGyk-tx8d>

# INTRODUCCION AL REVERSING CON IDA PRO DESDE CERO PARTE 53 KERNEL

Contents

[INTRODUCCION AL REVERSING CON IDA PRO DESDE CERO PARTE 53 KERNEL 1](#_Toc40962117)

[IRP 1](#_Toc40962118)

[IOCURRENTSTACKLOCATION 3](#_Toc40962119)

[MAJOR FUNCTION TABLE 8](#_Toc40962120)

<https://drive.google.com/open?id=1LvV_Ukhfg53LY_ZaKgURlNisiuMmG3-_>

# INTRODUCCION AL REVERSING CON IDA PRO DESDE CERO PARTE 54 KERNEL.

Contents

[INTRODUCCION AL REVERSING CON IDA PRO DESDE CERO PARTE 54 KERNEL. 1](#_Toc40962331)

[PRACTICA DRIVER KERNEL. 1](#_Toc40962332)

[CreateFile 6](#_Toc40962333)

[HANDLE 7](#_Toc40962334)

<https://drive.google.com/open?id=1DGakpudHZHci6bKz6AOPx69IHdcNDq19>

# INTRODUCCION AL REVERSING CON IDA PRO DESDE CERO PARTE 55 KERNEL.

Contents

[INTRODUCCION AL REVERSING CON IDA PRO DESDE CERO PARTE 55 KERNEL. 1](#_Toc40962612)

[OTRO EJERCICIO KERNEL 1](#_Toc40962613)

[\_EPROCESS 2](#_Toc40962614)

[HIDING A PROCESS 9](#_Toc40962615)

<https://drive.google.com/open?id=1BwNwDXykBqmTTIq6K5zn-PnFOYdoyB-i>

# INTRODUCCION AL REVERSING CON IDA PRO - KERNEL EXPLOITATION PARTE 56 KERNEL.

Contents

[56-INTRODUCCION AL REVERSING CON IDA PRO - KERNEL EXPLOITATION. 1](#_Toc40962907)

[HACKSYS VULNERABLE DRIVER. 1](#_Toc40962908)

[Vulnerabilities Implemented 1](#_Toc40962909)

<https://drive.google.com/open?id=16n9lh2a64b4CQpLXH2mG9HZ7gFYdOgn7>

# INTRODUCCION AL REVERSING CON IDA PRO DESDE CERO PARTE 57- KERNEL

Contents

[INTRODUCCION AL REVERSING CON IDA PRO DESDE CERO PARTE 57- KERNEL 1](#_Toc40963026)

[HACKSYS – STACK OVERFLOW. 1](#_Toc40963027)

<https://drive.google.com/open?id=18zykp6HWXb9_Y7_Fz8WrnVeSdDpj2bG1>

# INTRODUCCION AL REVERSING CON IDA PRO DESDE CERO PARTE 58

Contents

[INTRODUCCION AL REVERSING CON IDA PRO DESDE CERO PARTE 58 1](#_Toc40963442)

[TOKEN STEALER 1](#_Toc40963443)

[RETORNO SIN BSOD 1](#_Toc40963444)

[KTHREAD 7](#_Toc40963445)

[KPROCESS 7](#_Toc40963446)

[EPROCESS 11](#_Toc40963447)

[ELEVACION A SYSTEM 18](#_Toc40963448)

# 

<https://drive.google.com/open?id=1_fAB9JRjVqaI5bXMoUjxVUWB_w9tYxe0>

# INTRODUCCION AL REVERSING CON IDA PRO DESDE CERO PARTE 59

Contents

[INTRODUCCION AL REVERSING CON IDA PRO DESDE CERO PARTE 59 1](#_Toc40963681)

[ARBITRARY OVERWRITE 1](#_Toc40963682)

[\_IO\_STACK\_LOCATION 4](#_Toc40963683)

[DEVICEIOCONTROL 6](#_Toc40963684)

[HAL Dispatch 10](#_Toc40963685)

<https://drive.google.com/open?id=1G234OwsnYkZKhpJVY4vxlX0X6fjEUSyt>

# INTRODUCCION AL REVERSING CON IDA PRO DESDE CERO PARTE 60

Contents

[INTRODUCCION AL REVERSING CON IDA PRO DESDE CERO PARTE 60 1](#_Toc40966381)

[USANDO HAL EN KERNEL. 1](#_Toc40966382)

[CTYPES 1](#_Toc40966383)

[NtQuerySystemInformation 8](#_Toc40966384)

[SYSTEM\_MODULE\_INFORMATION\_ENTRY 11](#_Toc40966385)

<https://drive.google.com/open?id=1QFhj79CMOb6_gDzSichPPd8_k2fubf2N>

# INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 61.

Contents

[INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 61. 1](#_Toc40964301)

[INTEGER OVERFLOW 1](#_Toc40964302)

<https://drive.google.com/open?id=1a-uX-6C5Bk2nLTWQuACnfMQ13uh156Kz>

# INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 62.

Contents

[INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 62. 1](#_Toc40965571)

[WINDOWS 10 1](#_Toc40965572)

[SMEP 1](#_Toc40965573)

[DESHABILITAR FIRMAS. 4](#_Toc40965574)

[CPUID 13](#_Toc40965575)

[RP++ 15](#_Toc40965576)

<https://drive.google.com/open?id=1_CnoKGee9O7cb_y6epzCd4jMLW7wHBv2>

# INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 63.

Contents

[INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 63. 1](#_Toc40965731)

[SEGMENTACION Y PAGINACION DE MEMORIA PARA ARQUITECURA x86 1](#_Toc40965732)

[Memoria Real también llamada Física o Memoria RAM. 1](#_Toc40965733)

[Memoria Virtual 1](#_Toc40965734)

[MODO REAL 3](#_Toc40965735)

[MODO PROTEGIDO 4](#_Toc40965736)

[CR3 4](#_Toc40965737)

<https://drive.google.com/open?id=1sDQrLBf9bRcfv9-a5YuHY_zaGkp6uL1t>

# INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 64.

Contents

[INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 64. 1](#_Toc40965951)

[Reversing para el desafío de Scada 1](#_Toc40965952)

[CVE-2013-0657 1](#_Toc40965953)

<https://drive.google.com/open?id=1WauG0U8FqPFF1ozeWhoeH_QpE-xS-TIw>

# INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 65.

Contents

[INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 65. 1](#_Toc40966121)

[TUTE DEL DESAFIO DE NICO PARA LA EKOPARTY 2018 -PARTE 1 1](#_Toc40966122)

<https://drive.google.com/open?id=1rxLrQNOdgF1aLiXTUwIv3LC05IcOKJi->

# INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 66.

Contents

[INTRODUCCIÓN AL REVERSING CON IDA PRO DESDE CERO PARTE 66. 1](#_Toc40966198)

[TUTE DEL DESAFIO DE NICO PARA LA EKOPARTY 2018 -PARTE 2. 1](#_Toc40966199)

<https://drive.google.com/open?id=1loW437Zt9w1RNPgFxloeanonpPpdrrxO>

# INTRODUCCION AL REVERSING CON IDA PRO DESE CERO PARTE 67.

Contents

[INTRODUCCION AL REVERSING CON IDA PRO DESE CERO PARTE 67. 1](#_Toc40966438)

[Un método que no habíamos visto para explotar una de las vulnerabilidades del HACKSYS driver PISANDO SEH en 32 BITS. 1](#_Toc40966439)

<https://drive.google.com/open?id=1MiNeE6EpjQ4B1Qz3T3H-drmCg5HbCpLx>

# FIN