|  |
| --- |
|  |

****

|  |
| --- |
| **Armadillo 8.x** |
| Usando las herramientas en los momentos indicados |
|  |
| Este pequeño tutorial expondrá herramientas de otros usuarios para enfrentarnos a un armadillo 8.x un poco especial con sdk |
|  |
| **Apuromafo** |
| **02/12/2015** |
|  |

Contenido

[*Introducción:* 2](#_Toc436818841)

[Protecciones en el Armadillo: 3](#_Toc436818842)

[Unpacking con Ollydbg+Script: 4](#_Toc436818843)

[Conclusión: 8](#_Toc436818844)

# *Introducción:*

Hola siempre que abro mi carpeta de verificar encuentro uno que otro armadillo, comparto otra mini historia

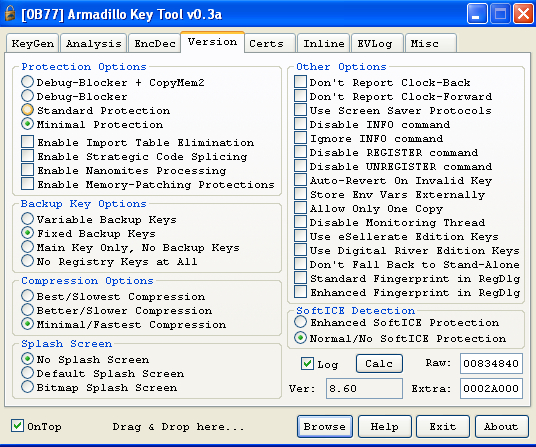
*Si quieres triunfar, no te quedes mirando la escalera. Empieza a subir, escalón por escalón, hasta que llegues arriba.*

|  |  |
| --- | --- |
| Programa | Network Security Auditing |
| Compañía | NSASOFT US, LLC |
| Descarga | http://www.nsauditor.com/network\_security/network\_security\_auditor.html |
| Tamaño | Setup: 10.6 MB / Programa: 6.1 MB |
| Víctima | Nsauditor.exe |
| Versión del Programa | 3.0.5.0 |
| Herramientas | OllyDbg y las que se necesiten para armadillo. |
| Packer/protector | Armadillo 8.x |
| Utilidad | Auditoría Web |
| Entorno | Windows 8.1 / Virtual Machine Windows XP sp3 |
| Compilador | Visual C/c++ |
| Objetivos | Desempacar /verificar si se puede registrar |
| Tutorial por | Apuromafo CLS |
| Fecha | 02-12-2015 |

El programa es full funcional, solo algunas nag/cosas varias desde armadillo, comparto este escrito porque tenía apuntado sus licencias (sym), pero veo que pasa los años y no actualizan los programas o mantienen los mismos niveles de licencia.

# Protecciones en el Armadillo:

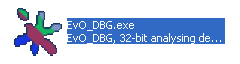
1. Analizando el Packer : Tool de Mr.exodia Armadillo Keytool (atk) [**https://github.com/mrexodia/akt**](https://github.com/mrexodia/akt)



Mis apuntes refieren algunos sym, pero el nivel de licencia es short v3 lv 10, requiere inline

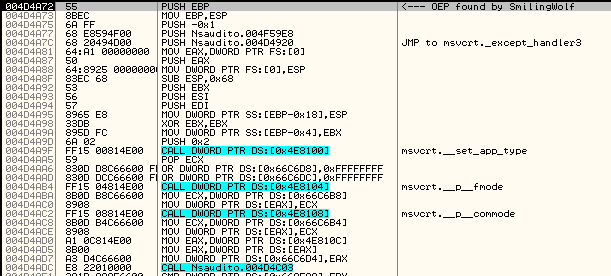
Datos actuales: Checksum (varios) salt: CDFD45F6 Level Short V3 Lv 10  
sym: 15686BBA - 1 user lic.//97B11F51 - 5 user lic. //90CE50DE - 25 user lic.//2E207468 - 50 user lic. //F1AC9001 - 100 user license

# Unpacking con Ollydbg+Script:

Windows xp sp3 en un entorno virtual Me propongo encontrar información relevante en un Evo Dbg

Hago uso de <https://forum.tuts4you.com/topic/36970-armadillo-factotum-universal-10/>

En el entrypoint, ejecuto script sin problema y en la ruta lo tenemos desempacado.

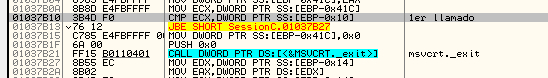


El programa no corre, porque verifica EnvironmentVariables cualquier error enviará a :



Primer llamado

, voy al lugar luego new origin y cambio el flag



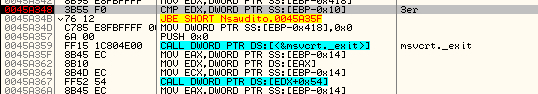


Al forzar el salto continua

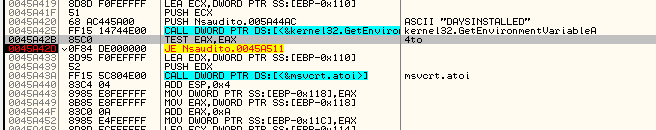
2do llamado del mismo lugar



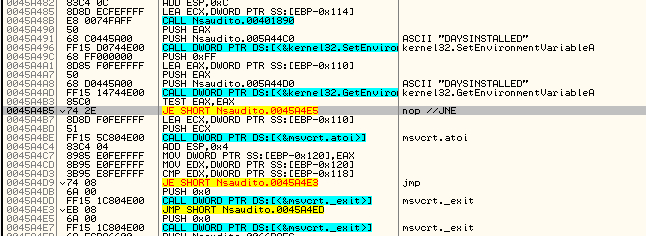
3er



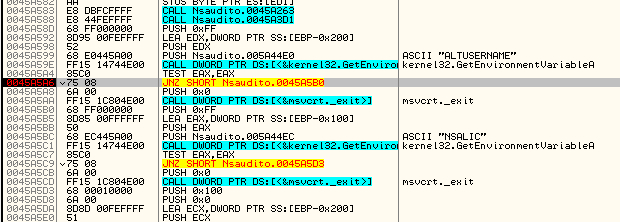
4to



5to y 6to

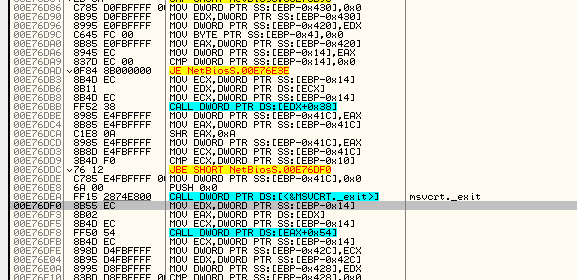


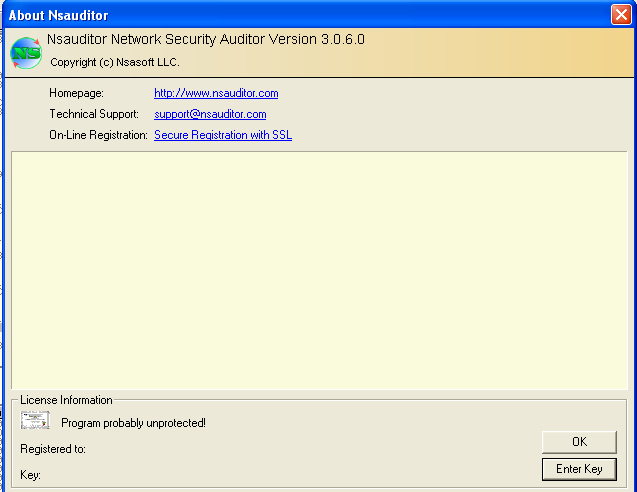
Se fuerza que salte



Con esos 8 parches el programa corre, en about refiere estar desprotegido

Aunque igual existen mas lugares





Al ir a la web, refiere <http://www.nsauditor.com/network_security/network_security_auditor_registered.html?utm_source=NSAUDITOR_APP&utm_medium=NSAUDITOR_APP_REG_URL&utm_content=No%20key!&utm_campaign=NSAUDITOR_APP#.Vl78ytJ96XY>



Verifico si corre en Windows 8.1 y tenemos el programa sin limitación:

# Conclusión:

Si fuera por resumir el escrito, tenemos un empacado con armadillo con muchas opciones, buen nivel de licencia, se puede inlinear y hacer mas, hoy solo pruebo el script a ver si funciona siempre a primera vista no veo secured section, pero basta con desempacar y está funcional.

Pd: Armadillo es un buen protector, el tema es cuando se quita la protección ya no es lo mismo de bueno, en este caso es mejor desempacar que registrar.

Saludos a toda la Lista de Crackslatinos. Apuromafo CLS

