

ReverseCraft

by gynvael.coldwind//vx

004 – Narzędzia i analizy

Strony projektu:

<http://re.coldwind.pl/>
<http://www.uw-team.org/>

Zanim zaczniemy...

Nie ma „jedynej słusznej” i „zawsze skutecznej” strategii analizowania aplikacji.

Każdy reverser ma własne metody, a i każda aplikacja jest inna.

Dlatego istotne jest aby poznać jak najwięcej metod, trików, strategii i podejść do reverse engineeringu!



Faza pierwsza:

REKONESANS

Plik wykonywalny

PEiD

ENT

skaner(y) AV

strings

PEView

PEExplorer

Zachowanie

Wireshark / Ethereal
Process Explorer
Process Monitor

Rozpakowywanie

LordPE / OllyDump
Import REConstructor



Faza druga:

ANALIZA BUDOWY

Disassembler + Debugger

IDA Pro
OllyDbg (+pluginy)



Faza trzecia:

M O D Y F I K A C J A

Edytory, edytory

Hexplorer

Hex Workshop

własne programy patchujące

Resource Hacker



Dziękuję za uwagę :)

Strony projektu:

<http://re.coldwind.pl/>
<http://www.uw-team.org/>