Features Business Explore Marketplace Pricing

This repository Search

Sign in or Sign up

enddo / awesome-windows-exploitation

Watch 208 Star 1,968 Fork 550

Code Issues 2 Pull requests 2 Projects 0 Insights

Join GitHub today

Dismiss

GitHub is home to over 20 million developers working together to host and review code, manage projects, and build software together.

Sign up

A curated list of awesome Windows Exploitation resources, and shiny things. Inspired by awesom

windows-exploitation windows-kernel windows-stack-overflows kernel-exploitation

56 commits 1 branch 0 releases 5 contributors Artistic-2.0

Branch: master New pull request Find file Clone or download

enddo Merge pull request #6 from nixawk/hotfix/readme_format_error …		Latest commit `1cc8ddb` on Mar 24, 2017
Source	Delete tut.txt	2 years ago

CONTRIBUTING.md	Create CONTRIBUTING.md	2 years ago
LICENSE	Create LICENSE	2 years ago
README.md	fix README.md format	a year ago

README.md

Awesome Windows Exploitation awesome

A curated list of awesome Windows Exploitation resources, and shiny things.

There is no pre-established order of items in each category, the order is for contribution. If you want to contribute, please read the guide.

Table of Contents

    - Fuzzysecurity
    - Securitysift
    - Whitehatters Academy
    - TheSprawl
    - Expdev-Kiuhnm
- Tools

Windows stack overflows

Stack Base Overflow Articles.

- Win32 Buffer Overflows (Location, Exploitation and Prevention) - by Dark spyrit [1999]
- Writing Stack Based Overflows on Windows - by Nish Bhalla's [2005]
- Stack Smashing as of Today - by Hagen Fritsch [2009]
- SMASHING C++ VPTRS - by rix [2000]

Windows heap overflows

Heap Base Overflow Articles.

- Third Generation Exploitation smashing heap on 2k - by Halvar Flake [2002]
- Exploiting the MSRPC Heap Overflow Part 1 - by Dave Aitel (MS03-026) [September 2003]
- Exploiting the MSRPC Heap Overflow Part 2 - by Dave Aitel (MS03-026) [September 2003]
- Windows heap overflow penetration in black hat - by David Litchfield [2004]
- Glibc Adventures: The Forgotten Chunk - by François Goichon [2015]
- Pseudomonarchia jemallocum - by argp & huku

- The House Of Lore: Reloaded - by blackngel [2010]
- Malloc Des-Maleficarum - by blackngel [2009]
- free() exploitation technique - by huku
- Understanding the heap by breaking it - by Justin N. Ferguson [2007]
- The use of set_head to defeat the wilderness - by g463
- The Malloc Maleficarum - by Phantasmal Phantasmagoria [2005]
- Exploiting The Wilderness - by Phantasmal Phantasmagoria [2004]
- Advanced Doug lea's malloc exploits - by jp

Kernel based Windows overflows

Kernel Base Exploit Development Articles.

- How to attack kernel based vulns on windows was done - by a Polish group called “sec-labs” [2003]
- Sec-lab old whitepaper
- Sec-lab old exploit
- Windows Local Kernel Exploitation (based on sec-lab research) - by S.K Chong [2004]
- How to exploit Windows kernel memory pool - by SoBeIt [2005]
- Exploiting remote kernel overflows in windows - by Eeye Security
- Kernel-mode Payloads on Windows in uninformed - by Matt Miller
- Exploiting 802.11 Wireless Driver Vulnerabilities on Windows
- BH US 2007 Attacking the Windows Kernel
- Remote and Local Exploitation of Network Drivers
- Exploiting Comon Flaws In Drivers
- I2OMGMT Driver Impersonation Attack

- Real World Kernel Pool Exploitation
- Exploit for windows 2k3 and 2k8
- Alyzing local privilege escalations in win32k
- Intro to Windows Kernel Security Development
- There’s a party at ring0 and you’re invited
- Windows kernel vulnerability exploitation
- A New CVE-2015-0057 Exploit Technology - by Yu Wang [2016]
- Exploiting CVE-2014-4113 on Windows 8.1 - by Moritz Jodeit [2016]
- Easy local Windows Kernel exploitation - by Cesar Cerrudo [2012]
- Windows Kernel Exploitation - by Simone Cardona 2016
- Exploiting MS16-098 RGNOBJ Integer Overflow on Windows 8.1 x64 bit by abusing GDI objects - by Saif Sherei 2017
- Windows Kernel Exploitation : This Time Font hunt you down in 4 bytes - by keen team [2015]
- Abusing GDI for ring0 exploit primitives - [2016]

Windows Kernel Memory Corruption

Windows Kernel Memory Corruption Exploit Development Articles.

- Remote Windows Kernel Exploitation - by Barnaby Jack [2005]
- windows kernel-mode payload fundamentals - by Skape [2006]
- exploiting 802.11 wireless driver vulnerabilities on windows - by Johnny Cache, H D Moore, skape [2007]
- Kernel Pool Exploitation on Windows 7 - by Tarjei Mandt [2011]
- Windows Kernel-mode GS Cookies and 1 bit of entropy - [2011]
- Subtle information disclosure in WIN32K.SYS syscall return values - [2011]
- nt!NtMapUserPhysicalPages and Kernel Stack-Spraying Techniques - [2011]

- SMEP: What is it, and how to beat it on Windows - [2011]
- Kernel Attacks through User-Mode Callbacks - by Tarjei Mandt [2011]
- Windows Security Hardening Through Kernel Address Protection - by Mateusz "j00ru" Jurczyk [2011]
- Reversing Windows8: Interesting Features of Kernel Security - by MJ0011 [2012]
- Smashing The Atom: Extraordinary String Based Attacks - by Tarjei Mandt [2012]
- Easy local Windows Kernel exploitation - by Cesar Cerrudo [2012]
- Using a Patched Vulnerability to Bypass Windows 8 x64 Driver Signature Enforcement - by MJ0011 [2012]
- MWR Labs Pwn2Own 2013 Write-up - Kernel Exploit - [2013]
- KASLR Bypass Mitigations in Windows 8.1 - [2013]
- First Dip Into the Kernel Pool: MS10-058 - by Jeremy [2014]
- Windows 8 Kernel Memory Protections Bypass - [2014]
- An Analysis of A Windows Kernel-Mode Vulnerability (CVE-2014-4113) - by Weimin Wu [2014]
- Sheep Year Kernel Heap Fengshui: Spraying in the Big Kids' Pool - [2014]
- Exploiting the win32k!xxxEnableWndSBArrows use-after-free (CVE 2015-0057) bug on both 32-bit and 64-bit - by Aaron Adams [2015]
- Exploiting MS15-061 Microsoft Windows Kernel Use-After-Free (win32k!xxxSetClassLong) - by Dominic Wang [2015]
- Exploiting CVE-2015-2426, and How I Ported it to a Recent Windows 8.1 64-bit - by Cedric Halbronn [2015]
- Abusing GDI for ring0 exploit primitives - by Diego Juarez [2015]
- Duqu 2.0 Win32k exploit analysis - [2015]

Return Oriented Programming

- The Geometry of Innocent Flesh on the Bone: Return-into-libc without Function Calls
- Blind return-oriented programming

- Sigreturn-oriented Programming
- Jump-Oriented Programming: A New Class of Code-Reuse Attack
- Out of control: Overcoming control-flow integrity
- ROP is Still Dangerous: Breaking Modern Defenses
- Loop-Oriented Programming(LOP): A New Code Reuse Attack to Bypass Modern Defenses - by Bingchen Lan, Yan Li, Hao Sun, Chao Su, Yao Liu, Qingkai Zeng [2015]
- Systematic Analysis of Defenses Against Return-Oriented Programming -by R. Skowyra, K. Casteel, H. Okhravi, N. Zeldovich, and W. Streilein [2013]
- Return-oriented programming without returns -by S.Checkoway, L. Davi, A. Dmitrienko, A. Sadeghi, H. Shacham, and M. Winandy [2010]
- Jump-oriented programming: a new class of code-reuse attack -by T. K. Bletsch, X. Jiang, V. W. Freeh, and Z. Liang [2011]
- Stitching the gadgets: on the ineffectiveness of coarse-grained control-flow integrity protection - by L. Davi, A. Sadeghi, and D. Lehmann [2014]
- Size does matter: Why using gadget-chain length to prevent code-reuse attacks is hard - by E. Göktas, E.Athanasopoulos, M. Polychronakis, H. Bos, and G.Portokalidis [2014]
- Buffer overflow attacks bypassing DEP (NX/XD bits) – part 1 - by Marco Mastropaolo [2005]
- Buffer overflow attacks bypassing DEP (NX/XD bits) – part 2 - by Marco Mastropaolo [2005]
- Practical Rop - by Dino Dai Zovi [2010]
- Exploitation with WriteProcessMemory - by Spencer Pratt [2010]
- Exploitation techniques and mitigations on Windows - by skape
- A little return oriented exploitation on Windows x86 – Part 1 - by Harmony Security and Stephen Fewer [2010]
- A little return oriented exploitation on Windows x86 – Part 2 - by Harmony Security and Stephen Fewer [2010]

Windows memory protections

Windows memory protections Introduction Articles.

- Data Execution Prevention
- /GS (Buffer Security Check)
- /SAFESEH
- ASLR
- SEHOP

Bypassing filter and protections

Windows memory protections Bypass Methods Articles.

- Third Generation Exploitation smashing heap on 2k - by Halvar Flake [2002]
- Creating Arbitrary Shellcode In Unicode Expanded Strings - by Chris Anley
- Advanced windows exploitation - by Dave Aitel [2003]
- Defeating the Stack Based Buffer Overflow Prevention Mechanism of Microsoft Windows 2003 Server - by David Litchfield
- Reliable heap exploits and after that Windows Heap Exploitation (Win2KSP0 through WinXPSP2) - by Matt Conover in cansecwest 2004
- Safely Searching Process Virtual Address Space - by Matt Miller [2004]
- IE exploit and used a technology called Heap Spray
- Bypassing hardware-enforced DEP - by Skape (Matt Miller) and Skywing (Ken Johnson) [October 2005]
- Exploiting Freelist[0] On XP Service Pack 2 - by Brett Moore [2005]
- Kernel-mode Payloads on Windows in uninformed
- Exploiting 802.11 Wireless Driver Vulnerabilities on Windows
- Exploiting Comon Flaws In Drivers

- Heap Feng Shui in JavaScript by Alexander sotirov [2007]
- Understanding and bypassing Windows Heap Protection - by Nicolas Waisman [2007]
- Heaps About Heaps - by Brett moore [2008]
- Bypassing browser memory protections in Windows Vista - by Mark Dowd and Alex Sotirov [2008]
- Attacking the Vista Heap - by ben hawkes [2008]
- Return oriented programming Exploitation without Code Injection - by Hovav Shacham (and others) [2008]
- Token Kidnapping and a super reliable exploit for windows 2k3 and 2k8 - by Cesar Cerrudo [2008]
- Defeating DEP Immunity Way - by Pablo Sole [2008]
- Practical Windows XP2003 Heap Exploitation - by John McDonald and Chris Valasek [2009]
- Bypassing SEHOP - by Stefan Le Berre Damien Cauquil [2009]
- Interpreter Exploitation : Pointer Inference and JIT Spraying - by Dionysus Blazakis[2010]
- Write-up of Pwn2Own 2010 - by Peter Vreugdenhil
- All in one 0day presented in rootedCON - by Ruben Santamarta [2010]
- DEP/ASLR bypass using 3rd party - by Shahin Ramezany [2013]
- Bypassing EMET 5.0 - by René Freingruber [2014]

Typical windows exploits

- Real-world HW-DEP bypass Exploit - by Devcode
- Bypassing DEP by returning into HeapCreate - by Toto
- First public ASLR bypass exploit by using partial overwrite - by Skape
- Heap spray and bypassing DEP - by Skylined
- First public exploit that used ROP for bypassing DEP in adobe lib TIFF vulnerability
- Exploit codes of bypassing browsers memory protections

- PoC’s on Tokken TokenKidnapping . PoC for 2k3 -part 1 - by Cesar Cerrudo
- PoC’s on Tokken TokenKidnapping . PoC for 2k8 -part 2 - by Cesar Cerrudo
- An exploit works from win 3.1 to win 7 - by Tavis Ormandy KiTra0d
- Old ms08-067 metasploit module multi-target and DEP bypass
- PHP 6.0 Dev str_transliterate() Buffer overflow – NX + ASLR Bypass
- SMBv2 Exploit - by Stephen Fewer
- Microsoft IIS 7.5 remote heap buffer overflow - by redpantz
- Browser Exploitation Case Study for Internet Explorer 11 - by Moritz Jodeit [2016]

Exploit development tutorial series

Exploid Development Tutorial Series Base on Windows Operation System Articles.

- Corelan Team
    - Exploit writing tutorial part 1 : Stack Based Overflows
    - Exploit writing tutorial part 2 : Stack Based Overflows – jumping to shellcode
    - Exploit writing tutorial part 3 : SEH Based Exploits
    - Exploit writing tutorial part 3b : SEH Based Exploits – just another example
    - Exploit writing tutorial part 4 : From Exploit to Metasploit – The basics
    - Exploit writing tutorial part 5 : How debugger modules & plugins can speed up basic exploit development
    - Exploit writing tutorial part 6 : Bypassing Stack Cookies, SafeSeh, SEHOP, HW DEP and ASLR
    - Exploit writing tutorial part 7 : Unicode – from 0x00410041 to calc
    - Exploit writing tutorial part 8 : Win32 Egg Hunting
    - Exploit writing tutorial part 9 : Introduction to Win32 shellcoding

  - Exploit writing tutorial part 10 : Chaining DEP with ROP – the Rubik’s Cube
  - Exploit writing tutorial part 11 : Heap Spraying Demystified

- Fuzzysecurity

  - Part 1: Introduction to Exploit Development
  - Part 2: Saved Return Pointer Overflows
  - Part 3: Structured Exception Handler (SEH)
  - Part 4: Egg Hunters
  - Part 5: Unicode 0x00410041
  - Part 6: Writing W32 shellcode
  - Part 7: Return Oriented Programming
  - Part 8: Spraying the Heap Chapter 1: Vanilla EIP
  - Part 9: Spraying the Heap Chapter 2: Use-After-Free
  - Part 10: Kernel Exploitation -> Stack Overflow
  - Part 11: Kernel Exploitation -> Write-What-Where
  - Part 12: Kernel Exploitation -> Null Pointer Dereference
  - Part 13: Kernel Exploitation -> Uninitialized Stack Variable
  - Part 14: Kernel Exploitation -> Integer Overflow
  - Part 15: Kernel Exploitation -> UAF
  - Part 16: Kernel Exploitation -> Pool Overflow
  - Part 17: Kernel Exploitation -> GDI Bitmap Abuse (Win7-10 32/64bit)
  - Heap Overflows For Humans 101
  - Heap Overflows For Humans 102
  - Heap Overflows For Humans 102.5

  - Heap Overflows For Humans 103
  - Heap Overflows For Humans 103.5

- Securitysift
  - Windows Exploit Development – Part 1: The Basics
  - Windows Exploit Development – Part 2: Intro to Stack Based Overflows
  - Windows Exploit Development – Part 3: Changing Offsets and Rebased Modules
  - Windows Exploit Development – Part 4: Locating Shellcode With Jumps
  - Windows Exploit Development – Part 5: Locating Shellcode With Egghunting
  - Windows Exploit Development – Part 6: SEH Exploits
  - Windows Exploit Development – Part 7: Unicode Buffer Overflows

- Whitehatters Academy
  - Intro to Windows kernel exploitation 1/N: Kernel Debugging
  - Intro to Windows kernel exploitation 2/N: HackSys Extremely Vulnerable Driver
  - Intro to Windows kernel exploitation 3/N: My first Driver exploit
  - Intro to Windows kernel exploitation 3.5/N: A bit more of the HackSys Driver
  - Backdoor 103: Fully Undetected
  - Backdoor 102
  - Backdoor 101

- TheSprawl
  - corelan - integer overflows - exercise solution
  - heap overflows for humans - 102 - exercise solution

- exploit exercises - protostar - final levels
- exploit exercises - protostar - network levels
- exploit exercises - protostar - heap levels
- exploit exercises - protostar - format string levels
- exploit exercises - protostar - stack levels
- open security training - introduction to software exploits - uninitialized variable overflow
- open security training - introduction to software exploits - off-by-one
- open security training - introduction to re - bomb lab secret phase
- open security training - introductory x86 - buffer overflow mystery box
- corelan - tutorial 10 - exercise solution
- corelan - tutorial 9 - exercise solution
- corelan - tutorial 7 - exercise solution
- getting from seh to nseh
- corelan - tutorial 3b - exercise solution

- Expdev-Kiuhnm
  - WinDbg
  - Mona 2
  - Structure Exception Handling (SEH)
  - Heap
  - Windows Basics
  - Shellcode
  - Exploitme1 (ret eip overwrite)
  - Exploitme2 (Stack cookies & SEH)

    - Exploitme3 (DEP)
    - Exploitme4 (ASLR)
    - Exploitme5 (Heap Spraying & UAF)
    - EMET 5.2
    - Internet Explorer 10 - Reverse Engineering IE
    - Internet Explorer 10 - From one-byte-write to full process space read/write
    - Internet Explorer 10 - God Mode (1)
    - Internet Explorer 10 - God Mode (2)
    - Internet Explorer 10 - Use-After-Free bug
    - Internet Explorer 11 - Part 1
    - Internet Explorer 11 - Part 2

Tools

Disassemblers, debuggers, and other static and dynamic analysis tools.

- angr - Platform-agnostic binary analysis framework developed at UCSB's Seclab.
- BARF - Multiplatform, open source Binary Analysis and Reverse engineering Framework.
- Binary Ninja - Multiplatform binary analysis IDE supporting various types of binaries and architecturs. Scriptable via Python.
- binnavi - Binary analysis IDE for reverse engineering based on graph visualization.
- Bokken - GUI for Pyew and Radare.
- Capstone - Disassembly framework for binary analysis and reversing, with support for many architectures and bindings in several languages.
- codebro - Web based code browser using clang to provide basic code analysis.

- dnSpy - .NET assembly editor, decompiler and debugger.
- Evan's Debugger (EDB) - A modular debugger with a Qt GUI.
- GDB - The GNU debugger.
- GEF - GDB Enhanced Features, for exploiters and reverse engineers.
- hackers-grep - A utility to search for strings in PE executables including imports, exports, and debug symbols.
- IDA Pro - Windows disassembler and debugger, with a free evaluation version.
- Immunity Debugger - Debugger for malware analysis and more, with a Python API.
- ltrace - Dynamic analysis for Linux executables.
- objdump - Part of GNU binutils, for static analysis of Linux binaries.
- OllyDbg - An assembly-level debugger for Windows executables.
- PANDA - Platform for Architecture-Neutral Dynamic Analysis
- PEDA - Python Exploit Development Assistance for GDB, an enhanced display with added commands.
- pestudio - Perform static analysis of Windows executables.
- Process Monitor - Advanced monitoring tool for Windows programs.
- Pyew - Python tool for malware analysis.
- Radare2 - Reverse engineering framework, with debugger support.
- SMRT - Sublime Malware Research Tool, a plugin for Sublime 3 to aid with malware analyis.
- strace - Dynamic analysis for Linux executables.
- Udis86 - Disassembler library and tool for x86 and x86_64.
- Vivisect - Python tool for malware analysis.
- X64dbg - An open-source x64/x32 debugger for windows.