# Windows Kernel Exploitation

N-part series on kernel exploitation in Windows environment demonstrating the exploit development phases, relevant mitigations and how they're bypassed.

- Part 1: Setting up the environment
- Part 2: Payloads
- Part 3: Stack Buffer Overflow (Windows 7 x86/x64)
- Part 4: Stack Buffer Overflow (SMEP Bypass)
- Part 5: Integer Overflow
- Part 6: NULL pointer dereference
- Part 7: Arbitrary Overwrite on Windows 7 x86
- Part 8: Arbitrary Overwrite on Windows 10 (TBD)

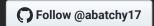
# Vulnhub Walkthroughs

- Vulnix
- PwnLab: init
- Kioptrix '
- Kioptrix 2
- Kioptrix 3
- Kioptrix 1.3 (#4)
- Kioptrix 2014 (#5
- Mr Robot
- LTR Scene '
- Wallaby's Nightmare









# Categories

- .Net Reversing
- Backdooring
- ▶ DefCamp CTF Qualifications 2017
- Exploit Development
- Kernel Exploitation
- Kioptrix series
- Networking
- OSCE Prep
- OSCP Prep
- OverTheWire Bandit
- OverTheWire Leviathan
- OverTheWire Natas
- Powershell
- Programming
- Pwnable.kr

- SLAE
- Shellcoding
- Vulnhub Walkthrough
- rant

# **Blog Archive**

## January 2018

- [Kernel Exploitation] 7: Arbitrary Overwrite (Win7 x86)
- [Kernel Exploitation] 6: NULL pointer dereference
- [Kernel Exploitation] 5: Integer Overflow
- [Kernel Exploitation] 4: Stack Buffer Overflow (SMEP Bypass)
- [Kernel Exploitation] 3: Stack Buffer Overflow (Windows 7 x86/x64)
- [Kernel Exploitation] 2: Payloads
- [Kernel Exploitation] 1: Setting up the environment

#### October 2017

- [DefCamp CTF Qualification 2017] Don't net, kids! (Revexp 400)
- [DefCamp CTF Qualification 2017] Buggy Bot (Misc 400)

#### September 2017

- [Pwnable.kr] Toddler's Bottle: flag
- [Pwnable.kr] Toddler's Bottle: fd, collision, bof
- OverTheWire: Leviathan Walkthrough

## August 2017

• [Rant] Is this blog dead?

#### June 2017

• Exploit Dev 101: Bypassing ASLR on Windows

#### May 2017

- Exploit Dev 101: Jumping to Shellcode
- · Introduction to Manual Backdooring

- Linux/x86 Disable ASLR Shellcode (71 bytes)
- Analyzing Metasploit linux/x86/shell bind tcp random port module using Libemu
- Analyzing Metasploit linux/x86/exec module using Ndisasm
- Linux/x86 Code Polymorphism examples
- Analyzing Metasploit linux/x86/adduser module using GDB
- Analyzing Metasploit linux/x86/adduser module using GDB
- ROT-N Shellcode Encoder/Generator (Linux x86)
- Skape's Egg Hunter (null-free/Linux x86)
- TCP Bind Shell in Assembly (null-free/Linux x86)

#### **April 2017**

• Shellcode reduction tips (x86)

#### March 2017

- LTR Scene 1 Walthrough (Vulnhub)
- Moria v1.1: A Boot2Root VM
- OSCE Study Plan
- Powershell Download File One-Liners
- How to prepare for PWK/OSCP, a noob-friendly guide

#### February 2017

- OSCP-like Vulnhub VMs
- OSCP: Day 30
- Mr Robot Walkthrough (Vulnhub)

### January 2017

- OSCP: Day 6
- OSCP: Day 1
- Port forwarding: A practical hands-on guide
- Kioptrix 2014 (#5) Walkthrough
- Wallaby's Nightmare Walkthrough (Vulnhub)

## December 2016

- Kiopritx 1.3 (#4) Walkthrough (Vulnhub)
- Kioptrix 3 Walkthrough (Vulnhub)
- Kioptrix 2 Walkthrough (Vulnhub)
- OverTheWire: Natas 17

#### November 2016

- OverTheWire: Natas 16
- OverTheWire: Natas 14 and 15
- Kioptrix 1 Walkthrough (Vulnhub
- PwnLab: init Walkthrough (Vulnhub)
- OverTheWire: Natas 12
- OverTheWire: Natas 11

#### October 2016

- Vulnix Walthrough (Vulnhub)
- OverTheWire: Natas 6-10
- OverTheWire: Natas 0-5
- OverTheWire: Bandit 21-26
- OverTheWire: Bandit 16-20
- OverTheWire: Bandit 11-15
- OverTheWire: Bandit 6-10
- OverTheWire: Bandit 0-5
- Introduction

Mohamed Shahat © 2018





