Dangling Pointer

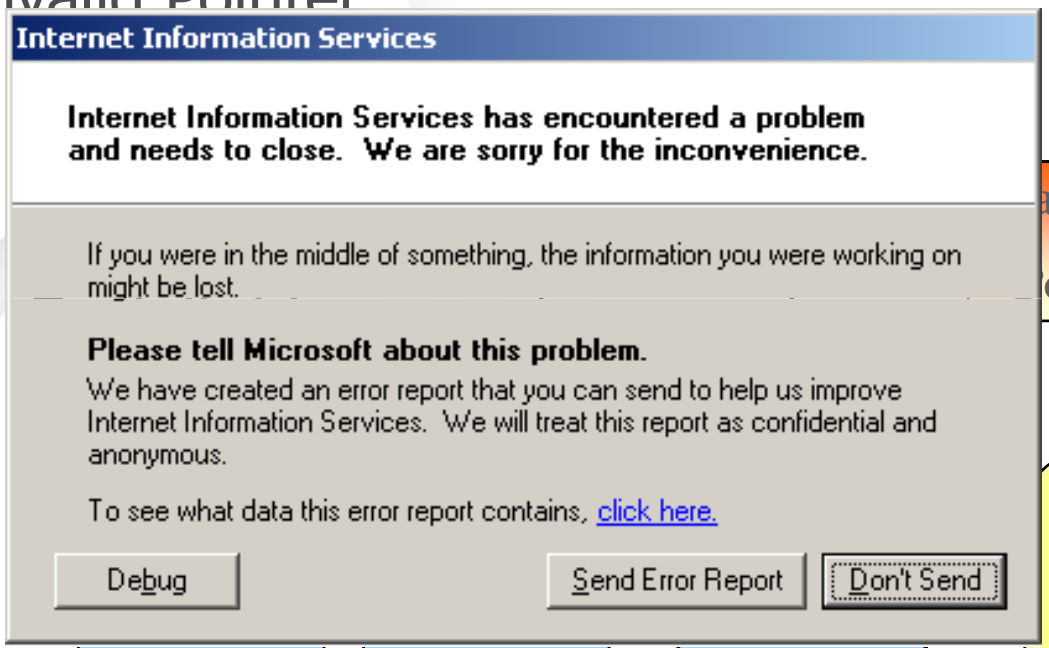
Jonathan Afek, 1/8/07, BlackHat USA

Table of Contents

watchfire

What is a Dangling Pointer?

Invalid Pointer:



angling

ointer

Object | Object | Object

Application Code:

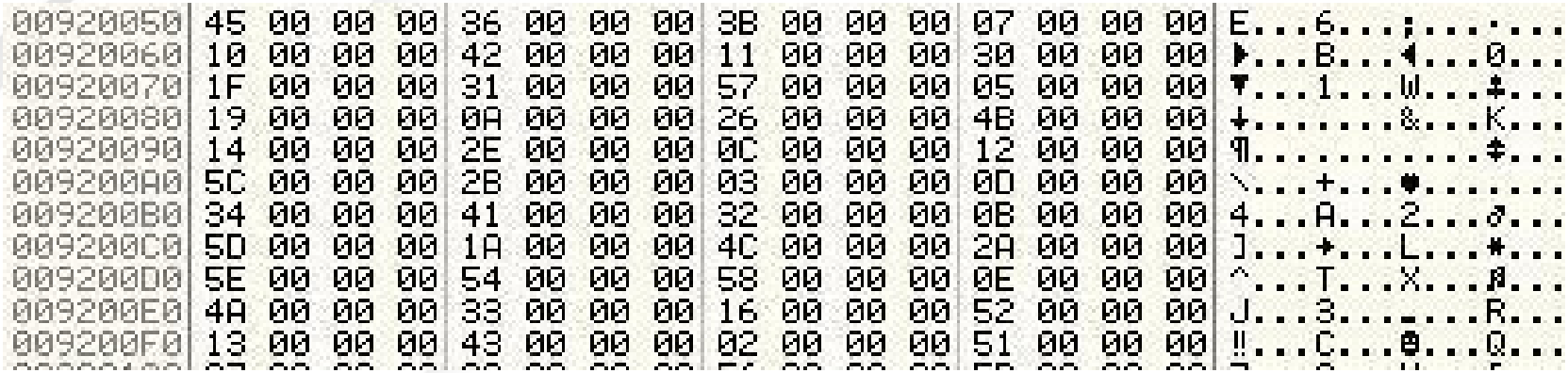
```
Pointer3 = new Object();
...
delete Pointer3;
...
Pointer3->func();
```

Overwrite the object

watchfire

What is a Dangling Pointer?

- Assembly
  - Memory Layout



```
00920050 45 00 00 00 36 00 00 00 3B 00 00 00 07 00 00 00 E...6...;.......
00920060 10 00 00 00 42 00 00 00 11 00 00 00 30 00 00 00 ►...B...◄...0...
00920070 1F 00 00 00 31 00 00 00 57 00 00 00 05 00 00 00 ▼...1...W...♣...
00920080 19 00 00 00 0A 00 00 00 26 00 00 00 4B 00 00 00 ↓.......&...K...
00920090 14 00 00 00 2E 00 00 00 0C 00 00 00 12 00 00 00 ¶.............↕...
009200A0 5C 00 00 00 2B 00 00 00 03 00 00 00 0D 00 00 00 \...+...♥.......
009200B0 34 00 00 00 41 00 00 00 32 00 00 00 0B 00 00 00 4...A...2...♂...
009200C0 5D 00 00 00 1A 00 00 00 4C 00 00 00 2A 00 00 00 ]...→...L...*...
009200D0 5E 00 00 00 54 00 00 00 58 00 00 00 0E 00 00 00 ^...T...X...♫...
009200E0 4A 00 00 00 33 00 00 00 16 00 00 00 52 00 00 00 J...3...▬...R...
009200F0 13 00 00 00 43 00 00 00 02 00 00 00 51 00 00 00 ‼...C...☻...Q...
```

  - Registers
  - Assembly code

watchfire

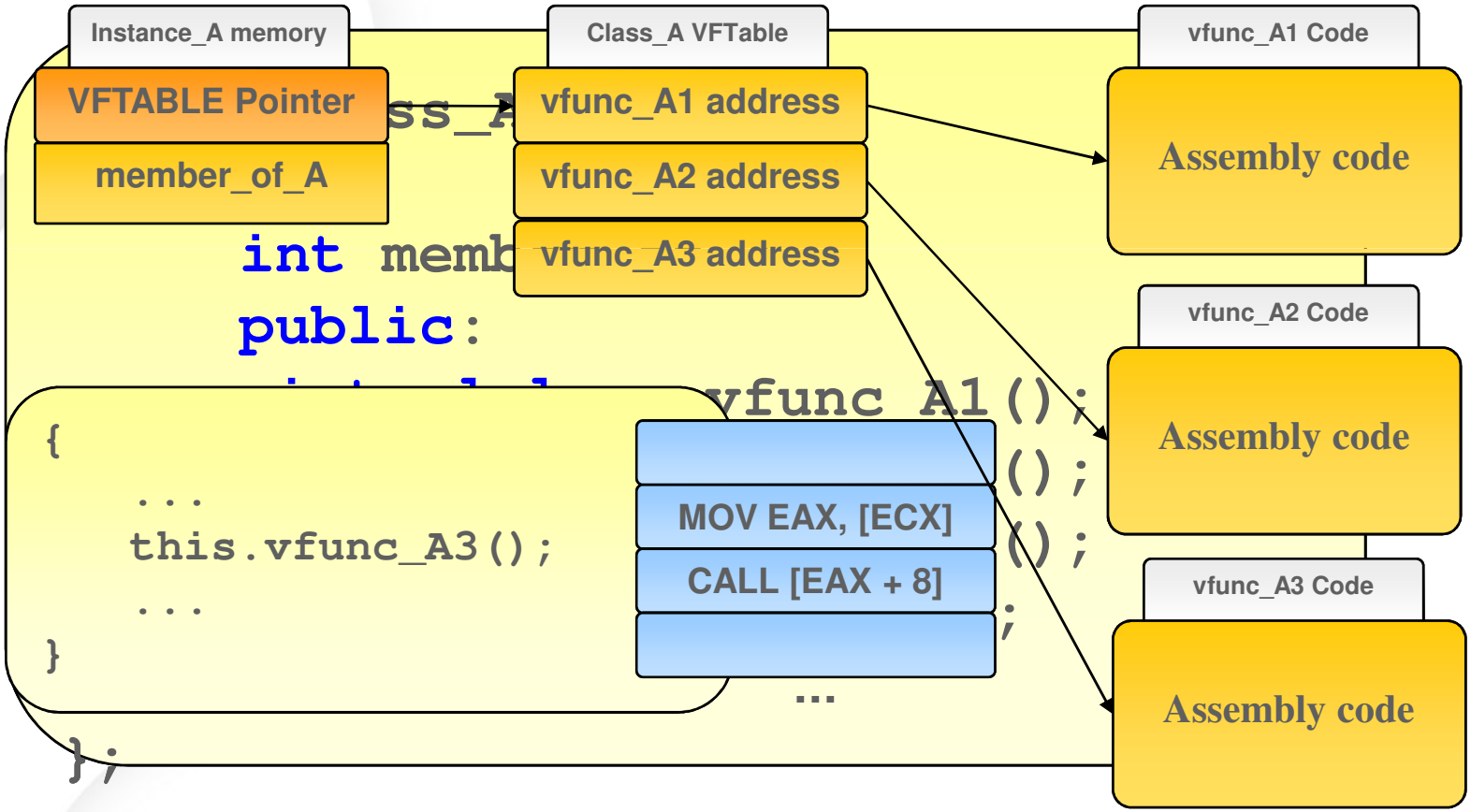
Where are We

- What is a Dangling Pointer?
- **Code Injection**
- Object Overwriting
- Demonstration
- Remediation
- Summary
- Q&A

watchfire

Code Injection – The Layout of an Object

- Class_A:



Code Injection – The Double Reference Exploit

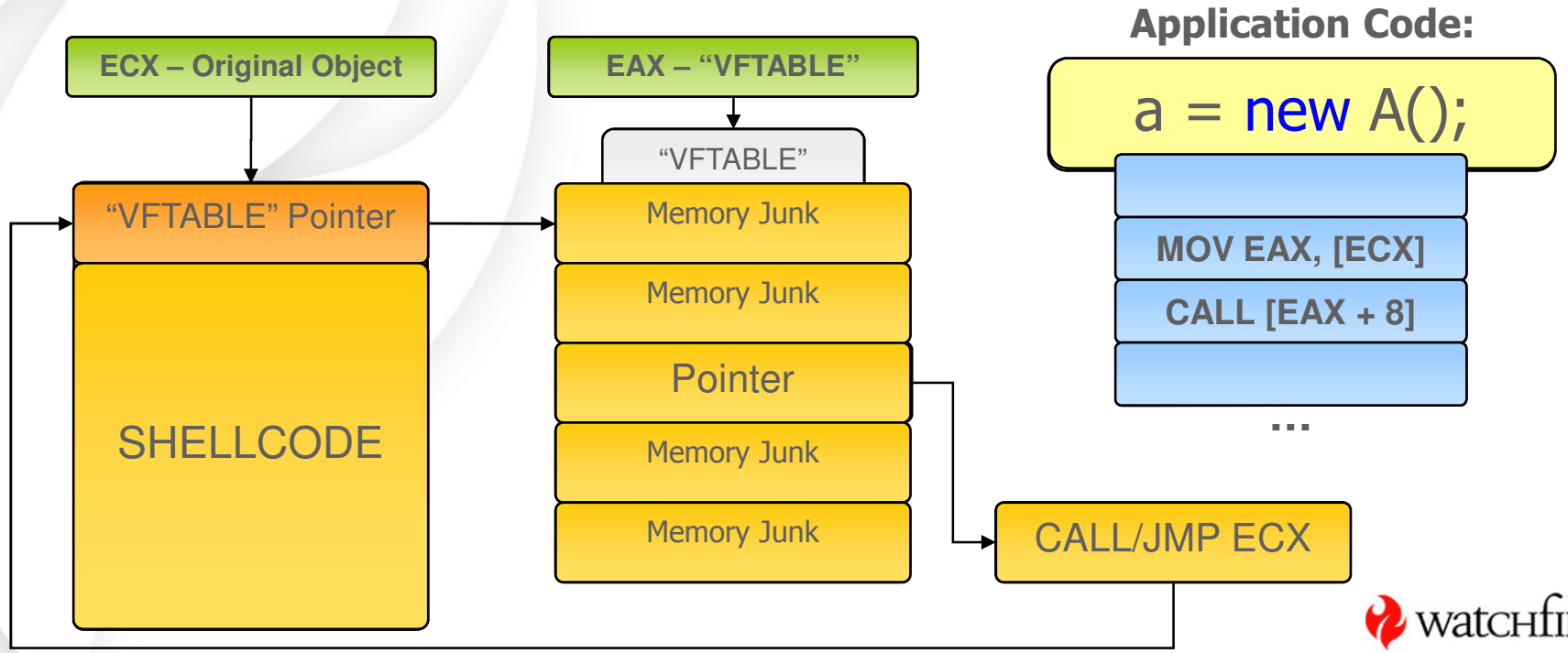
Exploit Overview:

- Free the Object
- Overwrite the Object
- Execute a Virtual Function

watchfire

Code Injection – The Double Reference Exploit

- *Object Allocated*
- *Object De-allocated*
- *Overwriting Object*
  - *Shellcode*
  - *Finding a "VFTable"*
- *VFunc3 Executed*



watchfire

Where are We

- What is a Dangling Pointer?
- Code Injection
- **Object Overwriting**
- Demonstration
- Remediation
- Summary
- Q&A

watchfire

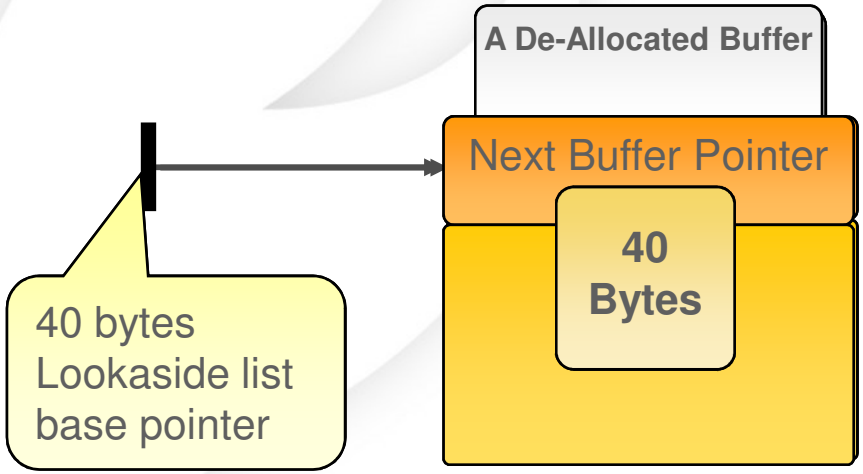
Object Overriding

- Allocation Implementation
  - C-Runtime heap
  - C-Runtime functions
    - Malloc
    - Free
    - New
    - Delete
    - Etc.

watchfire

Object Overriding

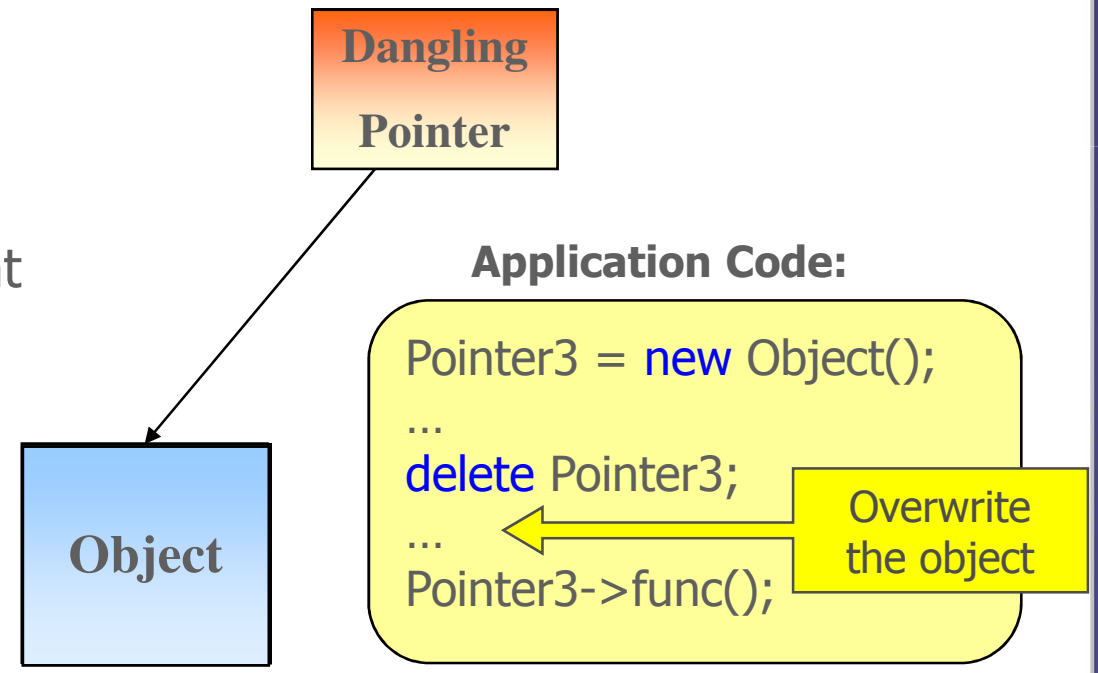
- Allocation implementation details
  - Lookaside List: Cache De-allcated Memory
    - A list for each size (8-1024) (8)
    - First Allocation Priority



watchfire

Object Overriding

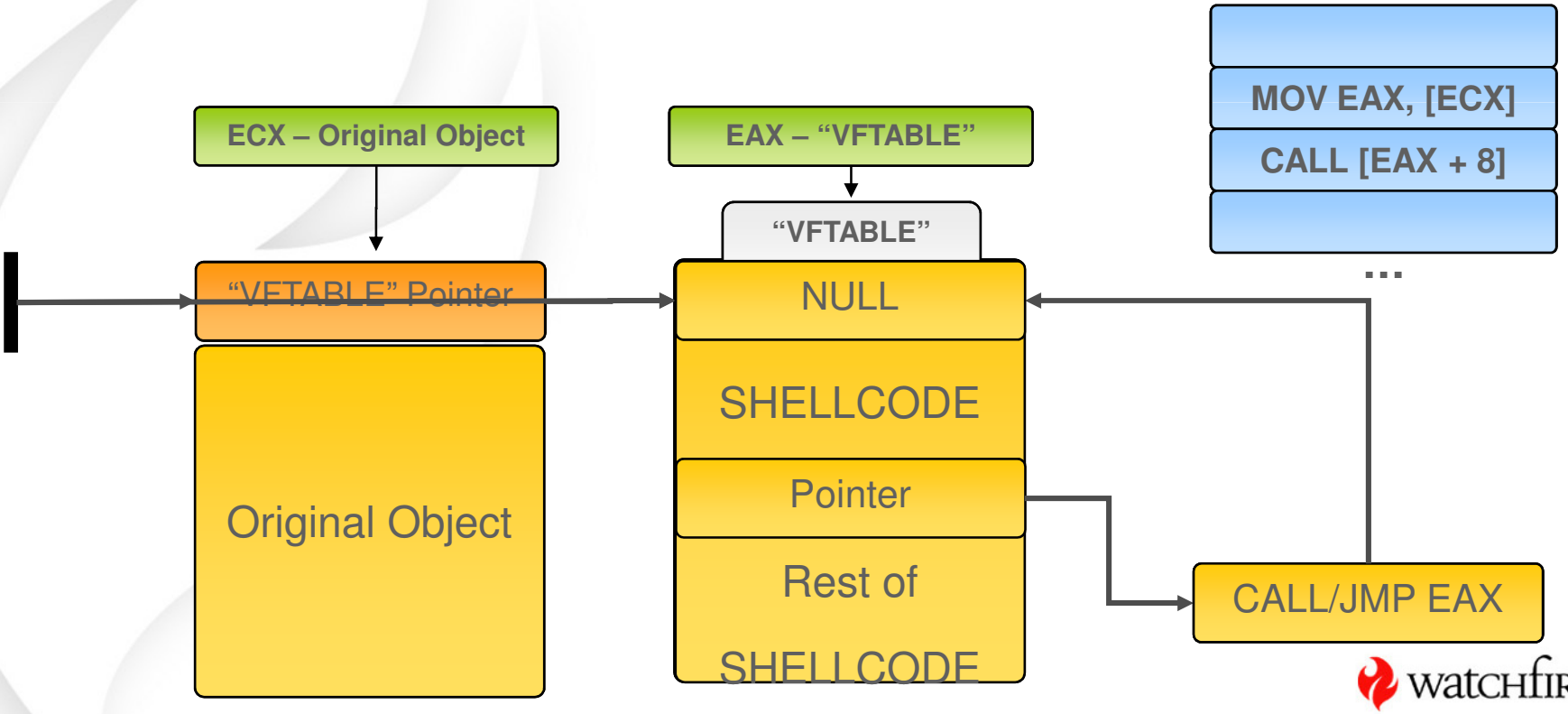
- Exploit Review
- Overwriting
  - Search for Allocations
    - Disassembly
    - Same Size
    - Controllable Content



watchfire

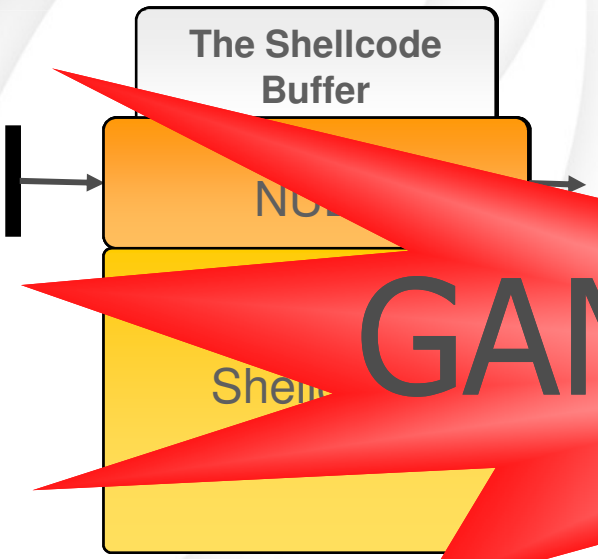
Object Overriding – The VFTABLE Exploit

- *Empty the Lookaside List*
- *Allocate a Buffer*
- *Insert Content*
- *Free the Buffer*
- *Free the Object*
- *Execute a VFunc*



Object Overriding – The Lookaside Exploit

- *Empty the Lookaside*
- *Allocate Two Buffers*
- *Insert Shellcode*
- *Free One Buffer*
- *Free the Other*
- *Free the Object*
- *Trigger the Bug*



GAME OVER!!!

watchfire

Object Overriding – The Lookaside Exploit

- Executing NULL – NO Problem

90	NOP
0000	ADD BYTE PTR DS:[EAX],AL
0000	ADD BYTE PTR DS:[EAX],AL
0000	ADD BYTE PTR DS:[EAX],AL
0F34	SYSENTER

watchfire

Summary

- Double Reference Exploit
  - Controllable First DWORD
  - Static Address
- VFTABLE Exploit
  - Controllable Allocations
  - No First DWORD
  - Static Address
- Lookaside Exploit
  - Controllable Allocations
  - No First DWORD
  - No Static Address
  - Destructor Execution

watchfire

Where are We

- What is a Dangling Pointer?
- Code Injection
- Object Overwriting
- **Demonstration**
- Remediation
- Summary
- Q&A

watchfire

Demonstration

- Putting it Together
  - De-Allocate
  - Inject
  - Trigger

watchfire

Where are We

- What is a Dangling Pointer
- Code Injection
- Object Overwriting
- Demonstration
- **Remediation**
- Summary
- Q&A

watchfire

Remediation

- Known Protection Mechanisms
  - NX Bit
  - ASLR
- VFTABLE Sanitation
- Safe Programming

watchfire

Summary

- Technical Background
  - Memory Allocations
  - Objects Implementation
- Exploits
  - Double Reference Exploit
  - VFTABLE Exploit
  - Lookaside Exploit
- Demonstration
  - Microsoft IIS 5.1
- Dangling Pointer
  - Only Object Oriented Objects

watchfire

More Information

- www.Watchfire.com

watchfire

Questions

- Ask Away…

watchfire