Heap Massage

* Traditional exploitation has become tougher

* On Linux... who knows how to do it?

* On Windows

  * XP SP2 made it tougher

    * Lookaside overwrites

    * Last chunk overwrite

  * Vista anybody?
Heap Exploitation

* Vista:
  * Lookaside lists are gone...
  * Welcome Low Fragmentation Heap (?)
  * ... and more security checks.
Heap Exploitation

* Lookaside lists are gone...
* Welcome Low Fragmentation Heap (?)
* ... and more security checks.
Heap Exploitation

- So... are heap exploits gone?
- No way! we love them! help them stay!

* So lets go back to basics...

What's after the vulnerable buffer, which if corrupted, will let an attacker gain code execution?

anybody?
Heap Massaging

* Code

* Sensitive information

* Pointers, structures, etc. that let us do a 4bw

* Class pointers

Protections

C++ Usage
Heap Massaging

* Heap block ordering is vital.

* We can't leave it to fate.

* Need to take control of the order of blocks.

* Learn more of the application.

* Find other commands that you can use.

* Find memory leaks.

* Ideally, build remote malloc(), free(), etc.
HeapDraw/HeapTracer

Limits: 1.082366-1.125270 0x0004ee1f-0x0004f327 (1288)
Limits: 1.082366-1.125270 0x0004ee1f-0x0004f327 (1288)
Heap Massaging

* google for “Heap Feng Shui” (Alex Sotirov)

* HeapDraw/HeapTracer and a few more tools

(soon) http://oss.coresecurity.com