18.1.2017, Sec-Meetup Kassel

HEAP SPRAYING EINFÜHRUNG

Gliederung

- Einführung
- Stringallokationen
- Grundlegendes Skript
- Heap Spray Skript
- Exploit
- Derzeitige Schutzmaßnahmen

Motivation / Warum?

- Verständnis von Heap-Exploits
- Heute noch zahlreich zu finden

Einführung

```
1   // Stack
2   char text1[] = "Meetup";
3
4   // Data Segment
5   const char* text2 = "Meetup";
6
7   // allocate memory on the heap.
8   // use "free" to avoid memory zombies.
9   char *text = (char*) malloc(strlen("Meetup") + 1 );
```

Einführung

- Für die Einführung: Windows XP
- x86 32bit
- IE

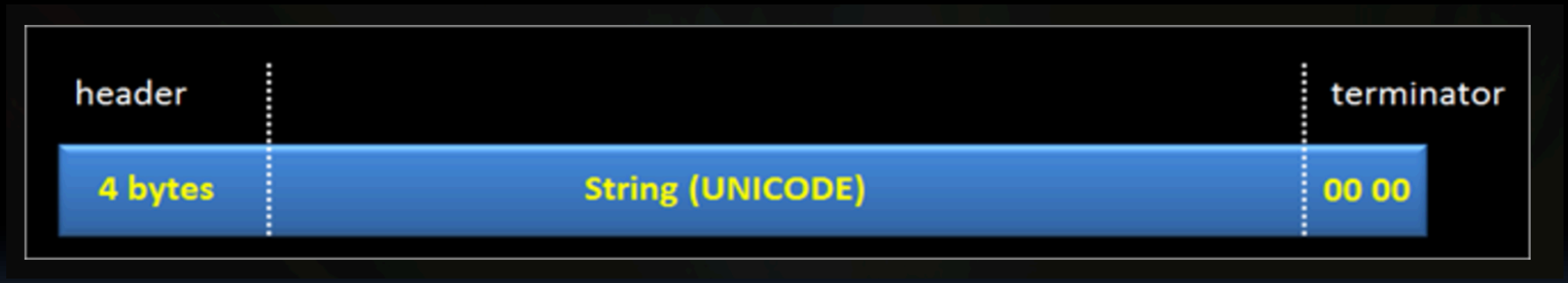
Einführung

2 Arten von Heaps:

- Default Heap: malloc
- Beliebig weitere Dynamic Heaps: HeapCreate

(weitere Infos https://msdn.microsoft.com/en-us/library/ms810603.aspx, abgerufen am 18.1.2017)

String Allokationen



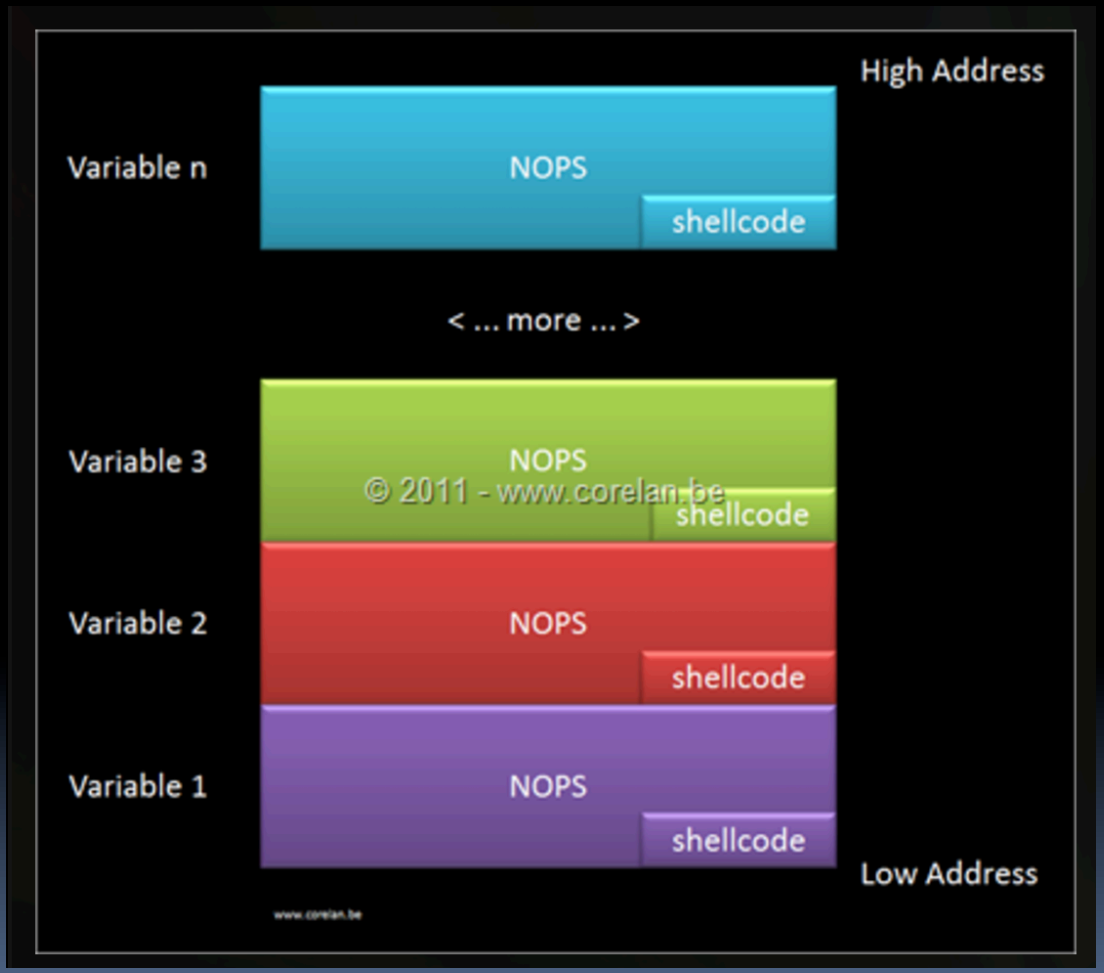
Entnommen https://www.corelan.be/index.php/2011/12/31/exploit-writing-tutorial-part-11-heap-spraying-demystified/, 17.01.2017

String Allokationen

- Heap Chunk Header

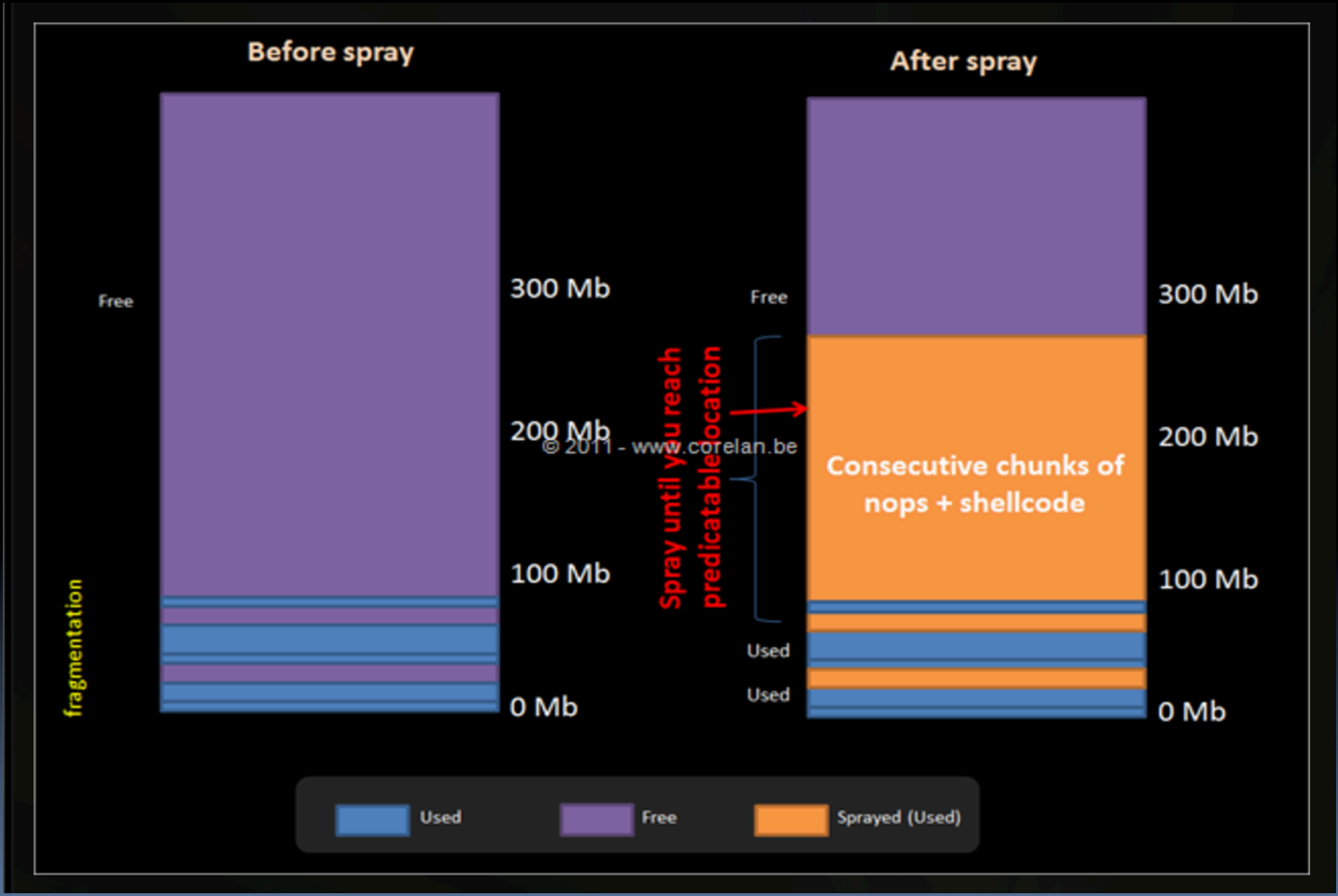
Entnommen https://www.corelan.be/index.php/2011/12/31/exploit-writing-tutorial-part-11-heap-spraying-demystified/, 18.01.2017

Grundlegendes Skript



Entnommen
https://www.corelan.be/index.php/2011/12/31/exploit-writing-tutorial-part-11-heap-spraying-demystified/,
17.01.2017

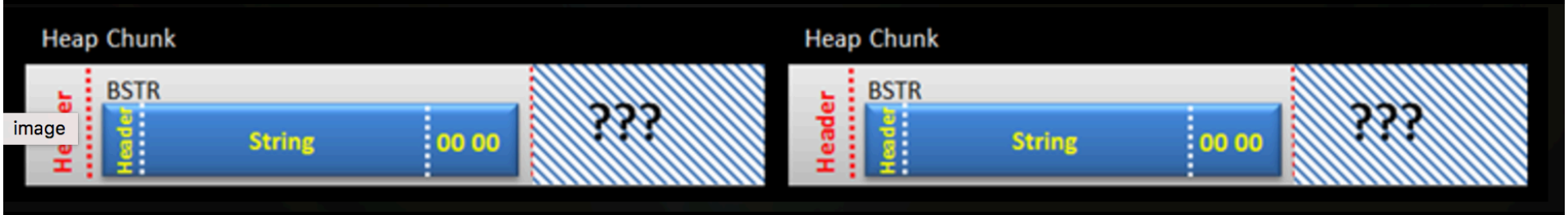
Grundlegendes Skript



Entnommen https://www.corelan.be/index.php/2011/12/31/exploit-writing-tutorial-part-11-heap-spraying-demystified/, 17.01.2017

Grundlegendes Skript

Zu vermeiden:



image

Entnommen https://www.corelan.be/index.php/2011/12/31/exploit-writing-tutorial-part-11-heap-spraying-demystified/, 17.01.2017

Strukturiertes Vorgehen

- Heap Feng Shui (https://www.youtube.com/watch?v=eoFWIh4waoo, und folgende Videos, abgerufen 17.1.2017)

Tools Heap-Spraying

- HeapLib2 (ungetestet: http://blog.ioactive.com/2013/11/heaplib-20.html, abgerufen 17.1.2017)

Schutzmaßnahmen (Heap)

- Nozzle (https://www.microsoft.com/en-us/research/publication/nozzle-a-defense-against-heap-spraying-code-injection-attacks/ , abgerufen 17.1.2017)
- BuBBle (http://cd80.ca/files/bubble.pdf, abgerufen 17.1.2017)
- EMET (https://support.microsoft.com/de-de/kb/2458544, abgerufen 18.1.2017)

Derzeitige Schutzmaßnahmen (Nicht-Heap spezifisch)

Unter anderem

- DEP
- ASLR
- SafeSEH

- Insbesondere aufgrund 64bit + ASLR schwer geworden

Aber ...

- 32bit Prozesse im Einsatz wo man sie gar nicht erwartet
- Antwort auf ASLR+DEP => JIT Spraying (http://blog.cdleary.com/2011/08/understanding-jit-spray/, abgerufen am 18.1.2017)
- MS16-039 Windows 10 64 bits Integer Overflow Heap Spraying aktuell (https://www.coresecurity.com/blog/ms16-039-windows-10-64-bits-integer-overflow-exploitation-by-using-gdi-objects, abgerufen am 18.1.2017)

Weiterführenden Links

- Heap Spraying
  https://www.corelan.be/index.php/2011/12/31/exploit-writing-tutorial-part-11-heap-spraying-demystified/
- WinDbg
  http://windbg.info/doc/1-common-cmds.html
- Aktuelle Situation
  http://security.stackexchange.com/questions/59307/heap-spray-against-64-bit-processes-possible

Zusammenfassung

- Einführung
- Stringallokationen
- Grundlegendes Skript
- Heap Spray Skript
- Exploit
- Aktuelle Situation