

Forum:[Hack Forums](#)

Thread: [Are stack overflows still effective?](#)

Ov3rf10w - November 30, 2014, 1:41 pm

I'm new in software security.

I've noticed that compilers have something called stack smashing protection, which stops you from overflowing fully through the stack on the compiled program.

Are stack overflows dying or are they still effective nowadays??

-Hyperion - November 30, 2014, 5:42 pm

It is dying out in some stuff but remember 37% of Windows are still XP machines etc so stack overflow is still usable.

Goodies - November 30, 2014, 7:08 pm

It seems to me that heap attacks are rather more common than stack overflows, but you should have a working understanding of both.

Ich1 - December 1, 2014, 8:38 am

Overflows are still prevalent in today's world but like Goodies said, you might want to get more comfortable with heap overflows because you'll run into those more. Stack overflows, to me, tend to be easier because of how the stack is handled..compared to heap. If you understand stack overflows, heap overflows shouldn't be too hard for you.

Here's a nice little guide on the differences and properties of Stack vs Heap

http://gribblelab.org/CBootcamp/7_Memory_Stack_vs_Heap.html

Ov3rf10w - December 1, 2014, 10:14 am

(Dec 1, 2014 09:38 AM)Ich1 Wrote: [\[CITE\]](#) Overflows are still prevalent in today's world but like Goodies said, you might want to get more comfortable with heap overflows because you'll run into those more. Stack overflows, to me, tend to be easier because of how the stack is handled..compared to heap. If you understand stack overflows, heap overflows shouldn't be too hard for you.

Here's a nice little guide on the differences and properties of Stack vs Heap Alright thanks for the replies and thank you for that info site ?

K0FIN - December 1, 2014, 4:56 pm

Stack Overflows are still alive and well, most people say they aren't because of protection schemes (ASLR, DEP, Stack canaries, etc.) but they are. The heap is a very popular exploitation vector as well, it's just a different segment of memory that is used differently than the stack. I would suggest to anyone that learning both is basically required.

K4Fr - December 1, 2014, 10:54 pm

Basic stack smashing is definitely in decline. Some are still exploitable, but many are entirely mitigated. And to be pedantic, the stack and heap are in the same segment, but are different regions within that segment. Segment has a technical meaning. Stack overflows are mostly mitigated by canaries and a general lack of flexibility in terms of what you can clobber. DEP and ASLR matter, but you usually do not even get to them (usually other mitigations stop you from even getting to the point of being blocked by DEP or ASLR). Heap overflows happen, but use after free and type

confusion are often easier to find. Stack overflows can be easier or harder depending on the details.

gizmodo - *December 3, 2014, 9:14 am*

Good to know this, I really appreciate the expert opinions.