Presentation Notes

Note: Anything you don't understand and can find on here - www.google.com

Segments & Sections
http://www.cirosantilli.com/elf-hello-world/#section-vs-segment
http://nairobi-embedded.org/040_elf_sec_seg_vma_mappings.html
http://www.roman10.net/2012/11/28/an-intro-to-elf-file-formatpart-2-sections-and-segments/
https://github.com/cirosantilli/notes/blob/master/stack-overflow/section-vs-segment.md
https://systemoverlord.com/2017/03/19/got-and-plt-for-pwning.html
https://www.technovelty.org/linux/plt-and-got-the-key-to-code-sharing-and-dynamic-libraries.html

Stack v Heap
http://net-informations.com/faq/net/stack-heap.htm
https://stackoverflow.com/questions/79923/what-and-where-are-the-stack-and-heap
http://www.programmerinterview.com/index.php/data-structures/difference-between-stack-and-heap/
https://www.gribblelab.org/CBootCamp/7_Memory_Stack_vs_Heap.html

X86 Registers
https://www.swansontec.com/sregisters.html
http://www.cs.virginia.edu/~evans/cs216/guides/x86.html
https://en.wikipedia.org/wiki/FLAGS_register
http://programmingethicalhackerway.blogspot.com.au/2015/07/the-complete-guide-of-assembly-registers.html
http://www.eecg.toronto.edu/~amza/www.mindsec.com/files/x86regs.html

Memory Corruption
https://azeria-labs.com/process-memory-and-memory-corruption/ ARM Tutorial
https://sploitfun.wordpress.com/2015/06/26/linux-x86-exploit-development-tutorial-series/
https://sploitfun.wordpress.com/2015/06/23/integer-overflow/ Might be useful?

Stack Overflows
http://phrack.org/issues/49/14.html
https://dhavalkapil.com/blogs/Buffer-Overflow-Exploit/
https://blog.techorganic.com/2015/04/10/64-bit-linux-stack-smashing-tutorial-part-1/
https://sploitfun.wordpress.com/2015/05/08/classic-stack-based-buffer-overflow/

Format Strings
https://crypto.stanford.edu/cs155/papers/formatstring-1.2.pdf
http://codearcana.com/posts/2013/05/02/introduction-to-format-string-exploits.html
https://www.exploit-db.com/docs/english/28476-linux-format-string-exploitation.pdf

Heap Overflows
https://www.win.tue.nl/~aeb/linux/hh/hh-11.html
http://homes.soic.indiana.edu/yh33/Teaching/I433-2016/lec13-HeapAttacks.pdf Complex but good!
http://www.mathyvanhoef.com/2013/02/understanding-heap-exploiting-heap.html
https://www.sans.edu/student-files/presentations/heap_overflows_notes.pdf

Protections
https://msdn.microsoft.com/en-us/library/windows/desktop/ff966508(v=vs.85).aspx
https://www.exploit-db.com/docs/english/17914-bypassing-aslrdep.pdf
https://en.wikipedia.org/wiki/Address_space_layout_randomization#Linux
https://www.corelan.be/index.php/2009/09/21/exploit-writing-tutorial-part-6-bypassing-stack-cookies-safeseh-hw-dep-and-aslr/

http://tk-blog.blogspot.com.au/2009/02/relro-not-so-well-known-memory.html
http://blog.siphos.be/2011/07/high-level-explanation-on-some-binary-executable-security/

ROP
https://en.wikipedia.org/wiki/Return-oriented_programming
https://www.exploit-db.com/docs/english/28479-return-oriented-programming-(rop-ftw).pdf
https://ropemporium.com/guide.html
http://codearcana.com/posts/2013/05/28/introduction-to-return-oriented-programming-rop.html
https://tc.gtisc.gatech.edu/cs6265/2016/l/lab07-rop/README-tut.txt
https://blog.skullsecurity.org/2013/ropasaurusrex-a-primer-on-return-oriented-programming
https://www.corelan.be/index.php/2010/06/16/exploit-writing-tutorial-part-10-chaining-dep-with-rop-the-rubikstm-cube/
https://sploitfun.wordpress.com/2015/05/08/bypassing-nx-bit-using-return-to-libc/

For the more difficult challenges I may provide my _other_ slide set that covers ret2libc.