EN.650.631 Ethical Hacking Home Work #2a

Recent examples such as [1] remind us that knowledge of core computer science courses is not a requirement to become an expert hacker. The only real requirements are a tenacious spirit and an analytical mind. Given these facts, please use your available resources to perform the below tasks.

1. Given the assembly language (64-bit Linux) code supplied to you, please explain the code.
2. Convert the supplied assembly language code into shellcode. What are the 3 steps that should be followed to transform assemble language code into shellcode?
3. Before using the shellcode, you should test it. Write C code to directly test your shellcode. Hint…this is step #3 from question #2.
4. Demonstrate the capability of your shellcode by modifying an existing Metaspolit payload or stand alone program with your shellcode (i.e., instead of executing the meterpreter or reverse tcp functionality, execute your shellcode). Then use this modified payload in any Linux exploiting module or program against the appropriate vulnerable remote target.

In a 5-minute (or less) video, explain and illustrate the results from your work above. You can work in groups of no more than two. Please email to Lanier.Watkins@jhuapl.edu and put **EN.650.431 and** both student names and in subject

References:

[1] A. Greenberg. "iPhone Super-Hacker Comex, Let Go From Apple, Goes To Work For Google". Forbes Online Magazine, April 24, 2013. Available at: http://www.forbes.com/sites/andygreenberg/2013/04/24/iphone-super-hacker-comex-let-go-from-apple-goes-to-work-for-google/#fe1536a60528