Texas Tech University
Computer Science Department
Digital Forensics – Reverse Engineering
Spring 2018, Individual Assignment 1, 10% of the final Mark
Due Date: TBA

NOTE: Perform all parts on your VM and minilab. There might be some dangerous and malicious activities that may harm your computer.

Part 1) [30% of the 10% marks] Visit the following link and analyze the pdf file along with the doc file without executing them. You will need to find relevant tools and commands for analyzing a doc file.

https://blog.didierstevens.com/2015/08/28/test-file-pdf-with-embedded-doc-dropping-eicar/

What to submit: A report along with some snapshots showing your analysis and finding.

Part 2) [30% out of 10% marks] Visit the following Website and do the "Bandit" (for the beginners) for all levels.

http://overthewire.org/wargames/bandit/

What to submit: A report along with some snapshots showing how you have done each level.

Part 3) [40% of the 10% marks] Analyze the malicious PDF given in the following link (also uploaded to the gitHub)

https://countuponsecurity.com/2014/09/22/malicious-documents-pdf-analysis-in-5-steps/

Cautions: PLEASE HANDLE THE MALICIOUS PDF FILE WITH CARE. DO NOT CLICK ON IT. DOWNLOAD IT INTO YOUR MINI-VIRTUAL LAB AND ANALYZE IT THERE WITHOUT EXECUTING IT.

Your job is to investigate the content of this malicious file. Using the PDF analyzing tools offered by the REMnux tool, address the following questions/activities:

1. Report the number of objects in the file.
2. Determine whether the file is compressed or not.
3. Determine whether the file is obfuscated or not.
4. Find and Extract JavaScript.
5. De-obfuscate JavaScript.
6. Extract the shell code.
7. Create a shell code executable
8. Analyze shell code and determine what is does.

For a quick tutorial on using the PDF analyzer tools offered by REMnus, you may review the following link:

https://countuponsecurity.com/2014/09/22/malicious-documents-pdf-analysis-in-5-steps/

What to Submit:

Submit a report addressing the above 8 questions and step-by-step on how you have done the process and which tools are used and how.

Happy Hacking