Advanced Security 2 – DT282-4, DT211-4 and DT228-4
Assignment 1 – 15%

Part A
Security has gained a lot of importance in the last few years. It is now a topic of conversation in nearly all walks of life. People with skills who can solve security problems are being sought after by government, private companies and society at large. In this assignment you will be required to research on the skills, certifications and training you will require to be a security expert. List your findings in one or two pages. Hint: start by looking at security job advertisements and reports such as http://goo.gl/c5zikq and http://goo.gl/4s5aAe.

Discuss why there is a shortage of security personnel worldwide. What measures/actions should be taken to address this shortage? Do you think you have enough skills to be a security expert? If no what are you missing and if yes what are your strengths?

Part B
There are a lot of technical explanations on why most of software we rely on is insecure. This has led to efforts being devoted in writing and producing software with no or very few errors. However, it is also true that to write secure code/software requires a lot of effort. And when writing secure code/software is applied in software industry everything becomes not only expensive but takes a lot more time. Therefore, with time to market and cost of software development being two of the most significant parameters in producing software, the software industry takes these parameters lightly or ignores them.

In this part, you will be required to test and identify security flaws using any two static code analysis tools such as https://goo.gl/VvlkFj. While these tools do not provide 100% guarantee, they can identify most of the security flaws. Use one programs from your labs or assignments you did in third or fourth year. The submission in this part will be a list of identified security flaws in the code.

Part C
Note: It is important when you are working these exercises to understand your social and legal responsibility to TUDublin and other users of its network. The ethical and legal ramifications are important to be understood in the context of the learning environment.

Google Hacking – Efficient use of Search Engines
Google hacking involves using advanced operators and security mind in the Google search engine to locate specific strings of text within search results. Understanding these Google hacking methods and techniques is an important skill for the penetration tester. In this assignment you will be required to investigate the use of the following:

1. Basic Operators:

+	-	~	.
*	“”	|	OR

2. Advanced Operators:

Allintext	allintitle	allinurl	cache
Define	filetype	info	intext
Intitle	inurl	link	related
Site	numrange	daterange	

For each operator give two examples of its usage. When it is used alone and in combination with other operator(s). Finally, comment if it is possible to achieve the same results without using operators given above.
Using the list of operators above identify if there are any equivalent operators that can be used in Bing (repeat the above exercise)? List ten new search engines giving their advantage(s) or disadvantages over Google or Bing

Part D

Security engineers see the world differently than other engineers. Instead of focusing on how the systems work, they focus on how the systems fail, how they can be made to fail, and how to prevent or protect against those failures. Most software vulnerabilities don’t ever appear in normal operations, only when an attacker deliberately exploits them. So security engineers need to think like attackers. This mindset is difficult to teach, and may be something you are born with or not. But in order to train people possessing the mindset, they need to search for and find security vulnerabilities again and again and again. And this is true regardless of the domain. Good Cryptographers discover vulnerabilities in other’s algorithms and protocols. Good software security experts find vulnerabilities in other’s code. Good airport security designers figure out new ways to subvert airport security.

Vulnerabilities are weaknesses in the system design, implementation, software or code, or the lack of a mechanism. Vulnerabilities and weaknesses are common with software mainly because there isn't any perfect software or code in existence. Vulnerabilities in software can be found in: firmware, operating systems, configuration files, application software and patches.

An exploit refers to a piece of software, tool, or technique that takes advantage of a vulnerability that leads to privilege escalation, loss of integrity, or denial of service on a computer system.

In this part of the assignment, you will be required to search for vulnerabilities that are found in applications, network, and protocols. Identify ten vulnerabilities and find exploits that can take advantage of these vulnerabilities. You will be required to

demonstrate how two exploits work. Please note that some of the exploits are malicious take care when demonstrating.

Submission Guidelines:

1. Report
   a) Each student will be required to submit a report of at most 5 to 10 pages.
   b) For each part write your findings in one or two pages.
   c) Upload your report in the Brightspace.

2. Demo
   a) Lab Demo will be in Week 5 and Week 6.

References

1. http://www.bbc.co.uk/news/uk-england-hereford-worcester-17118464, (Date of last access 29 Jan. 18).
2. http://www.bbc.co.uk/news/uk-england-coventry-warwickshire-16855572, (Date of last access 29 Jan. 18).
3. Johnny Long, 2005, Google Hacking for Penetration Testers, Syngress.
4. Johnny Long, Jack Wiles, Scott Pinzon and Kevin D. Mitnick, 2008, No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing.