Advanced Security 2 – DT211-4 and DT228-4

Assignment 1 – 20%

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

Part A
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.

Write a report of at most five pages for this part of the assignment which will be merged with report from other parts. No screen dumps.

Part B

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.

Part C

Demonstrate the use of Fingerprinting Organizations with Collected Archives (FOCA) - https://goo.gl/4LuVcl.

Part D

In this part of the assignment you will be required to list six different major vulnerability databases in use currently in vulnerability research. Finally, include in your report (video, software or shell command) related to finding vulnerabilities and implementing exploits that you think the rest of the class may find useful when they join the workforce as penetration testers or ethical hackers.

Each student will be required to submit a report of at most five pages describing what you have achieved in this assignment. Upload your report in Webcourses on or before 7th March 2016. The presentations for this assignment will be done in the lab on the 7th March 2016.

References

1. Information Assurance Analysis Technology Center, http://iac.dtic.mil/iatac/download /vulnerability_assessment.pdf, (Date of last access 22nd February 2012).
2. http://www.bbc.co.uk/news/uk-england-hereford-worcester-17118464, (Date of last access 22nd February 2012).
3. http://www.bbc.co.uk/news/uk-england-coventry-warwickshire-16855572, (Date of last access 22nd February 2012).
4. Johnny Long, 2005, Google Hacking for Penetration Testers, Syngress.
5. Johnny Long, Jack Wiles, Scott Pinzon and Kevin D. Mitnick, 2008, No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing.