

Advanced Security 2 – DT211-4, DT228-4 and DT282-4

Security Tools - (15%)

Over the last two decades security has become one of the most important issues in the Information Communication Technology landscape of most organisations. Organisations need security in order to ensure that their information processing systems are reliable. While Operating Systems provide some primitive security services, these are not enough to organisations expected to maintain a higher standard of data confidentiality, integrity and availability. Therefore, we have been witnessing a proliferation of security tools which provide additional security services to the information processing systems. Most of these security tools are used for checking and reporting the state of the systems and in some cases solving identified problems. Some security tools go a step further in the sense that they have sinister motives of deceiving users. We have reached a stage where it is extremely difficult to determine if the use of a particular security tool is legal or not. To make matters interesting legislators are busy making laws that react to public opinion and in some cases without a lot of thought on their implications to end users and developers. Therefore, even using some of the security tools for research is as uncertain as hackers seem to be with the law.

In this assignment you will be required to do the following:

1. Using Kali Linux (<https://www.kali.org/>) investigate the use of security tools it provides. Explore the working of any two tools (<https://tools.kali.org/tools-listing>) that you haven't used it before. You will be required to demonstrate the working of two security tools of your choice.
2. Use Metasploit (<http://www.metasploit.com/>) to demonstrate how vulnerabilities can be exploited. You may wish to use Metasploitable (<https://information.rapid7.com/metasploitable-download.html>). Make sure to Update Metasploit with the latest vulnerabilities.
3. Use Damn Vulnerable Web App (DVWA) which is a PHP/MySQL web application that is damn vulnerable to demonstrate how web applications can be hacked with two examples.
4. Finally, write a report (**Maximum 2 pages**) discussing the impact of laws in the use of security tools. Discuss whether it is ethical or not to carry out the experiments you have been doing, if not then how you should go about carrying the same experiments in the future. Are there any benefits in terms of organisation systems security improvements when we use security tools?

Submission Guidelines:

1. Demo
 - a. Create 5 to 8 PowerPoint slides (1 or 2 slides for each part)
 - b. Lab Demo will be in Week 11 and Week 12 and you have to verbally describe your presentation slides and content of your assignment.
2. Each student will be required to submit a report of at most 2 pages which will discuss the impact of laws in the use of security tools.

Make sure you upload your report through the Brightspace.

References

1. <http://www.securityfocus.com/>
2. <http://sectools.org/>
3. <http://www.security-database.com/toolswatch/>
4. <http://www.securitytube.net/>
5. Peter Sommer, Criminalising hacking tools, *Digital Investigation* 3(2): 68-72 (2007)