

**Advanced Security**

**Assignment 2**

**DT211C**

**BSc in Computer Science**

**Tim Browning**

**C14519547**

School of Computing

Dublin Institute of Technology

**Q1. Write a report 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?**

Security tools are a threat against digital information and IT assets. The tools use internal and external, malicious and accidental attacks on a system. There is an abundance of security tools; they are normally open source applications, which attack different areas of a system:

Kali Linux is an open-source security package for hackers. Kali Linux can be installed in a machine as an Operating System. NMAP and ZenMAP are useful tools for the scanning phase of Ethical Hacking in Kali Linux. NMAP is a free utility tool for network discovery and security auditing. Network administrators could find it useful for tasks such as network inventory and host monitoring and to check service uptime. NMAP uses IP packets determine which hosts are available on the network.

Using these tools improperly can get you sued, jailed, or banned by your ISP. The best way to avoid this is to always secure written authorization from the target network. I think these security tools can be used by people to defend their networks and to block attacks. These tools can be dangerous in the wrong hands so I do not think they should be public. These tools are open source, which means they can add functionality to make the tool even better at hacking into systems.

Nmap does not have any features designed to crash target networks Nmap and does not send any corrupt packets.

Network administrators can benefit from these functionalities:

* Bypass firewall
* Scan the network for vulnerabilities
* Perform fast DNS lookup
* Scan a range of IPs

Metasploit is a penetration-testing framework. It is an authorized simulated attack on a computer system. Metasploit can help determine whether a system is vulnerable to attack if the defenses were sufficient. Metasploit lets the tester execute an illegal operation which include unescaped SQL commands, unchanged salts in source-visible projects and old hash or crypto functions. These operations would not be ethical if performed on another system without their consent.

The HACS use this service to address potential vulnerabilities, and stop adversaries. As part of this service, certified hackers typically conduct a simulated attack on a system searching for security weaknesses. They typically provide recommended remediation plans to address weaknesses discovered.

DVWA - Damn Vulnerable Web Application is a web application. Its goals are to aid security professionals to test their skills.

DVWA lets you create a hacking environment in a network. It lets you detect common vulnerabilities. Some of the most commons vulnerabilities of web platforms: SQLInjection, Cross Site Scripting. This application can help novice computer scientists to learn about hacking and security. Security is a role in which a lot of training and experience is required. It takes years to become an expert. DVWA is a great educational tool. This tool should be used for educational purposes and not criminal. It must be regulated.