Adam Afzal (15078108)

Penetration testing is a grey area in terms of ethics, upon introduction the majority would assume that we are hacking with malicious intent. Particularly, those who are in a field unrelated to computer science. This fear is completely natural, as the media portrays black hat hackers as delinquents who simply exist to gain financially (money laundering), or to force their political views onto somebody, a group of people, government, or organisation. There are of course those hackers who break into computer systems to show their fellow hackers that they are superior in knowledge, by challenging themselves to target and gain privileged access (usually admin rights) to a computer system, or to break into a network of a well renowned organisation (for example the Sony PlayStation security breach), they are able to convey some sort of technical prowess. This is known as trophy hunting. Trophy hunters are usually very loud and are easy to catch red handed, this is usually their intention, because hacking into a well-respected and acknowledged organisation usually makes the headlines.

A penetration testing toolkit can both be used responsibly (e.g. by a legitimate pen testing company) or a malicious user, the danger or ‘usefulness’ of the toolkit depends on the user’s knowledge. For example, one may keep a drawer full of sharp knives, but they only become effective if the user knows what he/she can utilise them for. We must make sure that our merchants are of a legitimate source and not simply hackers with ambitions to cause damage. We are developing a pen testing toolkit, there is no limit to what we can do, our tools will be used to break into parts or maybe fully into a company’s network, the risk we must mitigate is making sure that our tools are used in a controlled environment, and consult the purchasing company, in order to provide ourselves some consolation that the extent to which these tools are to be used are within the agreement of the penetration testers and the company to be ‘attacked’. If the attackers violate their agreement and use our tools to gain and maintain access to parts of a system that they were not authorised to, part of the scrutiny or responsibility may fall upon as a company.