

How to use the UK Computer Misuse Act on a Security Test



The Computer Misuse Act defines a series of offenses relating to hacking and thus the primary legislation of concern to penetration testers. The most significant amendment occurred in 2015 when the Act was updated to align with the Serious Crime Act 2015. Computer Misuse was added to the list of serious crimes with a maximum penalty for being found guilty increasing to a prison sentence of 14 years and the possibility of a fine. The computer misuse act relates to Unauthorised Access, Authorised Modification and Facilitation of Crime. It is therefore critical that authorisation to perform the security test is obtained in writing prior to the start of any test. Key points are:

- The duration of the authorization is obtained.
- That named individuals given authorization.

It is also critical that the person providing the authorization for the test is authorized provide the authorization.

Section 1

Section 1 of the computer misuse act relates to unauthorised access to a computer system. The conditions of this offence are:

- They cause a computer to perform any function with intent to secure access to any program or data held in any computer;
- The access they intend to secure unauthorised; and
- They know at the time when he causes the computer to perform the function that that is the case.

Section 2

Section 2 of the computer misuse act relates to Unauthorised access to computer materials with intent to commit a further crime. The conditions of this offence are:

- A person is guilty of an offence under this section if he commits an offence under section 1 above ("the unauthorised access offence") with intent:
 - to facilitate the commission of such an offence (whether by himself or by any other person);

Section 3

Section 3 of the computer misuse act relates to modification access to a computer system. The conditions of this offence are

- They do any unauthorised act in relation to a computer;
- At the time when they do the act, they know that it is unauthorised; and applies to:
 - To impair the operation of any computer;
 - To prevent or hinder access to any program or data held in any computer;
 - To impair the operation of any such program or the reliability of any such data;

Amendments

- The new offence in section 3ZA of the 1990 Act addresses the most serious cyber-attacks, for example those on essential systems controlling power supply, communications, food or fuel distribution. A major cyber-attack of this nature could have a significant impact, resulting in loss of life, serious illness or injury, severe social disruption or serious damage to the economy, the environment or national security.
- Section 42 of the Serious Crime Act now extends section 3A of the 1990 Act to include an offence of obtaining a tool for use to commit a section 1, 3 or 3ZA offence regardless of an intention to supply that tool – thus removing the requirement of the involvement, or intended involvement, of a third party and ensuring that the offence covers individuals acting alone.