

# Ethical Hacking & Countermeasures

The world's increasing reliance on the Internet has inevitably meant that computer crime is on the increase. Many companies are now so worried about the threat from cyber crime that they employ consultants to test the security of their computer networks. Legislation is currently being introduced that demands such security testing as part of the due diligence required in financial systems. As a result computer specialists skilled in the techniques of ethical hacking, and in the creation of the countermeasures necessary to protect systems from malicious hacking, are currently very much in demand.

An "ethical hacker" essentially evaluates the security of a computer system or network by simulating an attack by a malicious hacker. The process involves an active analysis of the system for any weaknesses, technical flaws or vulnerabilities. Security issues that are found will be presented to the system owner together with an assessment of their impact and often with a proposal for mitigation or a technical solution to the problem, a countermeasure. The systems owner must always give legal agreement before any testing is carried out.

This undergraduate programme aims to equip graduates with detailed knowledge of the nature of electronic attacks and methods that computer criminals use. Countermeasure techniques and strategies will be examined for their suitability against these attacks. Graduates from this programme will be equipped with the skills to analyse and secure computer systems and networks, to design countermeasures against criminal intrusion, penetration and hacking, and with the capability to continuously update and develop their knowledge and skills in this rapidly changing area.

The course is made up of 8 modules per year that are organised into themes. Some modules are single and are studied over one term, whilst others are double modules concerned with major topic areas studied over the entire academic year. The themes, together with the major topics, that you will be studying include;

**Ethical hacking and countermeasures** - This major theme looks at the nature of ethical computer hacking. This area will examine the tools and techniques that can be used, how systems can be tested and how the risks can be minimised.

**Professional Practice, Law and Ethics Legal issues.** This major theme looks extensively at legal and ethical issues. Also included in this area are project work and project management.

**Computer Networking** - This theme develops knowledge of wired and wireless networks. Topics include the basics of computer networking, via protocols and hardware such as routers and switches and also network management.

**Underlying exploitable technologies** – This area examines applications that are electronically exploitable, this includes databases, servers (such as http and E-Mail) and the operating systems that these application run on.

**Course**  
BSc (Hons) Ethical Hacking & Countermeasures

**UCAS Code**  
GG45/BSc EHC

**Duration**  
4 years full time



**Abertay  
University**  
Breaking Barriers

# Ethical Hacking & Countermeasures

**Year 1:** This is a foundation year providing an introduction to the fundamental principles. The modules include Team Based Problem Solving, Object Oriented Programming 1, Introduction to Ethical Hacking, The Personal Computer and Law

**Year 2:** In this year, fundamental topics are covered in greater depth. The modules include Computer Networking 1, Ethical Computer Hacking 1, Operating Systems, Dynamic XHTML, Scripting Technologies and Database Design Fundamentals.

**Year 3:** In this year, current issues are examined. The modules include Mobile Computing, Ethical Computer Hacking 2, Computer Networking 2, Forensic Computing and Group Project

**Year 4:** In the honours year, students will concentrate on a selected area or method of Ethical Hacking and Countermeasures. The modules include Network Management, Penetration Testing, Honours Project, Mobile Phone Technology and Communication Technology Law

## Career Opportunities

A potentially large job market is emerging for such a course. Currently, auditors are insisting that companies must have their network penetration tested for legal purposes (this is the case for the University of Abertay). The data protection act means that a network manager must take reasonable steps to protect personal data. All companies with "financial" considerations are also bound by banking acts such as Sarbanes-Oxley. The increase in this job market for graduates is likely to continue for the foreseeable future. Graduates from the BSc (Hons) Ethical Hacking and Countermeasures will have the necessary skills and background to become Penetration testers (a growing market), Ethical Hackers, Network Managers and Forensic Computing analysts.

## Course Accessibility

Students participating in the course may be involved in the following activities: team working, attending lectures and tutorials and undertaking practical work in laboratories. For advice on course accessibility, please contact John Petrie (Student Advisor) at [j.petrie@abertay.ac.uk](mailto:j.petrie@abertay.ac.uk) or telephone (01382) 308051.

## Further Information

Details of the entrance requirements can be found on our website. If you would like more information on the course, please contact the Student Recruitment Office (details at the bottom of the page).

*The information in this leaflet is correct at the time of going to print. As the University has a policy of regularly reviewing its courses, the course or content may be subject to change without prior notice.*

12/07

## Contact

For further information contact:  
Julie McEwan, Student Recruitment Office  
University of Abertay Dundee, Bell Street,  
Dundee DD1 1HG

**t:** 01382 308080 **f:** 01382 308081

**w:** [www.abertay.ac.uk/questions](http://www.abertay.ac.uk/questions)

**Abertay  
University**  
Breaking Barriers