Ethical Hacking Comes to Bedford College
Tuesday, 3 May – 9.00-12.30pm

There was a very impressive turn out of staff and students on the morning of Tuesday, 3 May to listen to Geraint Williams from the University of Bedfordshire share his experiences and demonstrate ethical hacking techniques. This lecture is one of an ongoing series of talks organised for the benefit of our Computing students and delivered by visiting industry experts. The group of forty students included both those studying part-time or full-time on the IT Networking and Security Foundation Degree, and Level 3 students studying on the BTEC Diploma or Extended Diploma in IT.

Geraint Williams is, without doubt, a leading expert and authority in the field of computer security and forensics, and is currently Infrastructure Manager and Senior Lecturer in the Computer Science and Technology faculty at the University of Bedfordshire.

The talk was designed as an introductory session on computer security and ethical hacking and included a demonstration of how a weakness in an operating system could be exploited to take over the machine - allowing the attacker to gain full control.

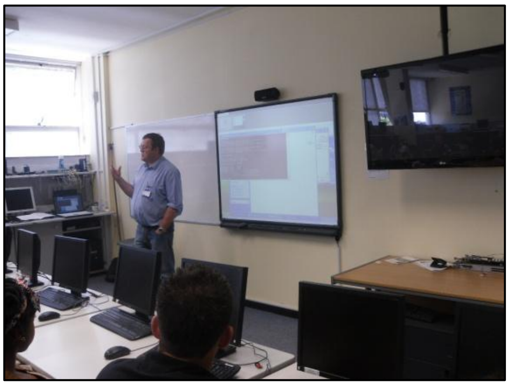
The main areas covered included – what we mean by computer security, phishing analysis, ethical hacking, a practical demonstration of hacking a computer and a brief discussion of wireless security.

The existence of the Internet and the wealth of resources it facilitates is so entwined with our daily lives that our IT systems and the data they hold can no longer live in isolation. The online society in which we now exist, demands that we stay connected - making cyber crime a lucrative and ever-present threat.

Providing overviews of the concepts of data security and discussing the common attack strategies, Geraint demonstrated the tools, social engineering techniques and operating systems vulnerabilities that hackers could use to exploit their victims.

Geraint then closed with a valuable insight into the careers opportunities available in the area of Security Testing - more commonly known as Ethical Hacking - and options for further study.

The talk was not only very educational and motivating but really 'hit the right' note - perfect content, level and length. The department suddenly seems to have a large number of students who want to develop their careers in computer security and forensics!



Further details of the topics covered in the talk are available on Bedford College's IT Employer website at http://www.bedfordtrainingservices.co.uk/

Richard Noble, BTEC National Diploma for IT Practitioners, said "I was surprised how much was covered in a short space of time and how detailed the information was. It gave me an insight into what an ethical hacker has to do, some of the tools and techniques that are used and how valuable ethical hackers are to businesses."

Summary of Topics Covered During Lecture and Demonstration

- ✓ **Computer Security**
  Geraint introduced the concept of computer security, why we need security and the fact that the concept extends beyond solely technical/hardware controls. The reasons why the Internet is insecure were examined and the terminology of the information security professional explained

- ✓ **Phishing Analysis**
  Geraint worked though an example of a phishing attack to show how the sender of an email can be identified even if the email header had been modified.

- ✓ **Ethical Hacking**
  The importance of understanding the legal issues associated with ethical hacking was discussed. Ethical hacking or penetration testing is used to test security countermeasures to ensure they are effectively working. This type of activity can only be done with the permission of the legal owner of the network. Geraint explained a hacker's approach to thinking through an attack - and the anatomy of attack.

- ✓ **Demonstration of Hacking a Computer**
  Geraint covered the principles laid out in the section on ethical hacking - following the stages a hacker would go through and using a security tester to prove a vulnerability that can be exploited. The demonstration involved the use of virtual machines to represent a target and an attacking system.

The stages included:

Mapping / Scanning - Using a piece of open source software that is available as a system administration tool to check network configurations, the network was scanned to identify machines, open ports and to enumerate the operating system and applications by using ‘banner grabbing’. The target machine was found to be running an old version of Windows XP with an old version of IIS (Microsoft's web server software). It is recognised that an operating system of this age is vulnerable to a RPC buffer overflow.

Attack / Gaining Access – Access was gained using a script that exploits the RPC buffer overflow vulnerability to create a remote backdoor to the target machine that can then be accessed using a Telnet client. Geraint then demonstrated the ability to now to create users and add them to the local Admin group. He also demonstrated the ability to remotely upload software to the target machine.

Maintaining Access – Once access had been gained and an account created, Geraint used a network based password recovery tool to retrieve the password hashes and then conduct a dictionary attack to crack the Administrator password. Geraint also installed an additional backdoor piggybacking on the web server - using malformed packets on port 80 as an ‘out of channel’ communication system.

Covering Tracks – Geraint discussed and demonstrated the use of Rootkits. Additional users were then deleted since he then had the Admin password. The possibility of modifying log files was then discussed – and, finally Geraint demonstrated it was easy to deface the web server’s home page!!#

- ✓ **Wireless Security**
  Finally, there was a short section covering wireless networking and security issues based on research Geraint is currently undertaking. Geraint also demonstrated some of the wireless tools that can be used in the configuration and testing of wireless networks – including Vistumbler (used to find networks) and Wi-Spy DBX (a spectrum analysis tool to monitor RF spectrum for noise).