



# Scottish Information Assurance Forum



## SEMINAR: Ethical Hacking Friday 31<sup>st</sup> August 2012

Room A, Stirling Enterprise Park, Kerse Road, Stirling, FK7 7RP

Registration: 09:15  
Event Start: 09:30  
Event Close: 15:30

The Scottish Information Assurance Forum is delighted to bring this seminar to our members in conjunction with Sec-1. Sec-1 is a leading Network Security Solutions company specialising in Security Testing and Training and will facilitate one of their Penetration Testing workshops:

### Workshop Content:

#### Introduction

- Understanding the threats to your organisation
- Recent attack trends
- Real world examples

#### Attacking the Network Perimeter

- Understanding "Attack Surface"
- A review of the top 5 remotely exploitable vulnerabilities
- Finding, exploiting and preventing: SQL Injection, Cross Site Scripting, Insecure Administrative Interfaces, File Upload and Host Configuration vulnerabilities
- Live demonstration of common attack techniques
- Using open source and free tools to discover flaws within your network perimeter
- Defending the network perimeter

#### Internal Attacks

- A review of the top 5 network vulnerabilities
- Live demonstration of common attack techniques
- Gaining domain administrator control in 15 minutes
- Using open source and free tools to identify and fix common vulnerabilities
- Defensive strategies

#### Penetration Testing

- Introduction to Penetration Testing
- Commissioning a Penetration Test
- What information to provide and what to expect
- Selecting a provider

**All tools used in the workshop are available post event**



### Top 5 Network Vulnerabilities

Measured by impact as well as prevalence of vulnerability, this list summarises the key findings:

- SQL Injection
- Insecure Administrative Interfaces
- Persistent Cross Site Scripting
- Insecure File Upload Vulnerabilities
- Weak Passwords