Higher National Unit specification: general information

Unit title: Ethical Hacking Fundamentals

Unit code: H1EP 34

Superclass:	CB
Publication date:	April 2012
Source:	Scottish Qualifications Authority
Version:	01

Unit purpose

This Unit aims to introduce candidates to the concepts and practical skills required in real life ethical hacking engagements. By the end of this Unit candidates should be aware of the importance of the role of IT security and be able to perform information gathering steps, system security testing, system exploits, and access maintenance/track covering techniques and suggest possible countermeasures within a security assessment report.

On completion of the Unit the candidate should be able to:

1 Perform target information gathering reconnaissance.
2 Perform system security vulnerability testing.
3 Perform system vulnerability exploit attacks.
4 Produce a security assessment report.

Recommended prior knowledge and skills

Access to this Unit will be at the discretion of the Centre. However, it is recommended that candidates should have some prior knowledge and skills in Computing/Information Technology/Networking. This may be evidenced by the possession of relevant National Units, HN Units or experience.

Credit points and level

1 Higher National Unit credit at SCQF level 7: (8 SCQF credit points at SCQF level 7*)

**SCQF credit points are used to allocate credit to qualifications in the Scottish Credit and Qualifications Framework (SCQF). Each qualification in the Framework is allocated a number of SCQF credit points at an SCQF level. There are 12 SCQF levels, ranging from Access 1 to Doctorates.*

General information (cont)

Core Skills

Opportunities to develop aspects of Core Skills are highlighted in the Support Notes of this Unit specification.

There is no automatic certification of Core Skills or Core Skill components in this Unit.

Context for delivery

If this Unit is delivered as part of a Group Award, it is recommended that it should be taught and assessed within the subject area of the Group Award to which it contributes.

Please Note: Centres are encouraged to ask candidates to sign an acceptable use policy when using ethical hacking tools.

Higher National Unit specification: statement of standards

Unit title: Ethical Hacking Fundamentals

Unit code: H1EP 34

Please refer to *Knowledge and/or Skills for the Unit* and *Evidence Requirements for the Unit* after the Outcomes.

Where evidence for Outcomes is assessed on a sample basis, the whole of the content listed in the Knowledge and/or Skills section must be taught and available for assessment. Candidates should not know in advance the items on which they will be assessed and different items should be sampled on each assessment occasion.

Outcome 1

Perform target information gathering reconnaissance.

Knowledge and/or Skills

- Use appropriate tools and/or techniques to gather relevant business information.
- Use appropriate tools and/or techniques to gather relevant individuals information.
- Use appropriate tools and/or techniques to gather relevant system information.

Outcome 2

Perform system security vulnerability testing.

Knowledge and/or Skills

- Demonstrate use of appropriate tools to scan and detect vulnerability issues.
- Use appropriate manual techniques to detect vulnerability issues.

Outcome 3

Perform system vulnerability exploit attacks.

Knowledge and/or Skills

- Use of appropriate tools and/or techniques to exploit system vulnerability.

Unit title: Ethical Hacking Fundamentals

Outcome 4

Produce a security assessment report.

Knowledge and/or Skills

- Structure requirements of a security assessment report.
- Use appropriate terminology expected in a security assessment report.
- Produce a report suitable for non-technical and technical staff.

Evidence Requirements for the Unit

Candidates will need evidence to demonstrate their Knowledge and/or Skills by showing that they can describe within a security assessment report their findings in relation to Outcomes 1, 2, 3 and 4.

The candidate will produce written evidence in the form of a security assessment report; the report must include as a minimum the following sections:

- Test Scope
- Rules of engagement
- An Executive Summary
- Vulnerability Report
- Proof of Exploit
- Remediation Report

Screen dumps or screen recording evidence of tools used in relation to Outcomes 1, 2, and 3 must be included as either part of the report or as individual items in a blog or portfolio.

Higher National Unit specification: support notes

Unit title: Ethical Hacking Fundamentals

This part of the Unit specification is offered as guidance. The support notes are not mandatory.

While the exact time allocated to this Unit is at the discretion of the centre, the notional design length is 40 hours.

Guidance on the content and context for this Unit

This Unit is designed to give candidates an opportunity to learn about the role of ethical hacking.

Candidates should learn that ethical hacking is a vital part of computing. Operating Systems, applications, network infrastructure components and business processes must be tested in order to insure security and minimise risk to the business and the end service user.

Candidates should learn about the hacker lifecycle and mentality of a determined hacker and use similar tools/techniques in order to protect business and the general public from malicious activity.

Candidates should learn about the importance of raising security awareness and the need to communicate at levels appropriate to the clients.

Guidance on the delivery of this Unit

There is only one assessment for this Unit. The report which can be based upon tests carried out on any of the following images provided should be written in a way that concentrates on findings and remediation strategy as these are the important aspects to business.

As ethical hacking or penetration testing as it is sometimes referred to, is a combination of practical skills and specialist system knowledge, it is vital that as many opportunities to learn from practical experiences are given as possible.

There are a number of useful resources already available online and can be used to allow for both the practical and theoretical areas to be fully explored.

These are as follows:

http://pynstrom.net/holynix.php — Test image and tutorials

https://github.com/adamdoupe/WackoPicko — Test image

http://blog.metasploit.com/2010/05/introducing-metasploitable.html — Test image designed to be used with metasploit.

http://code.google.com/p/owaspbwa/ — Test web applications

http://sourceforge.net/projects/lampsecurity/files/ — Test web applications and documentation.

http://www.damnvulnerablelinux.org/ — Test image.

http://www.badstore.net/ — Test image and documentation.

http://www.securitytube.net/ — Video demonstrations of tools and techniques

http://www.darknet.org.uk/ — Security tools, guides, whitepapers.

http://www.owasp.org/index.php/Main_Page — Tools, technical discussion, guides, test images and standards

http://www.mavensecurity.com/web_security_dojo/ — Open source training image.

http://www.darkreading.com/ — News, guides, blogs and slides.

http://www.offensive-security.com/metasploit-unleashed/Metasploit_Unleashed_Information_Security_Training — Online manual for metasploit.

Guidance on the assessment of this Unit

The assessment for Outcomes 1, 2, 3 and 4 are combined and further information is given in the guidance below.

Assessment Guidelines

Outcomes 1–4

There is only one assessment for this Unit covering Outcomes 1–4. The candidate should produce written evidence in the form of a security assessment report; the report must include as a minimum the following sections:

- Test Scope
- Rules of engagement
- An Executive Summary
- Vulnerability Report
- Proof of Exploit
- Remediation Report

The test scope should be determined by the lecturer, the candidate should obtain the scope by means of an interview or questionnaire.

During this process the candidate and lecturer should agree and sign off the rules of engagement.

The executive summary should be written with a target audience in mind of non advanced computer users at an executive level. Candidates may wish to make use of graphs, charts and other visual aids to identify business risks as a result of the vulnerabilities found.

The vulnerability report should be written with a target audience in mind of advanced technical support/developers and should include appropriate references to standard classification systems such as MITRE CVE, WASC or OWASP.

The proof of exploit section should provide enough general information for the recipients of the report to carry out the attack in order to re-create the vulnerability.

The remediation report should include short term/long term remediation recommendations.

Online and Distance Learning

If this Unit is delivered by open or distance learning methods, additional planning and resources may be required for candidate support, assessment and quality assurance.

Suitable test images must be provided and a mechanism for online support.

Opportunities for the use of e-assessment

E-assessment may be appropriate for some assessments in this Unit. By e-assessment we mean assessment which is supported by Information and Communication Technology (ICT), such as e-testing or the use of e-portfolios or social software. Centres which wish to use e-assessment must ensure that the national standard is applied to all candidate evidence and that conditions of assessment as specified in the Evidence Requirements are met, regardless of the mode of gathering evidence. Further advice is available in *SQA Guidelines on Online Assessment for Further Education (AA1641, March 2003).*

Opportunities for developing Core Skills

There is no automatic certification of Core Skills or Core Skill components in this Unit.

Disabled candidates and/or those with additional support needs

The additional support needs of individual candidates should be taken into account when planning learning experiences, selecting assessment instruments, or considering whether any reasonable adjustments may be required. Further advice can be found on our website **www.sqa.org.uk/assessmentarrangements**

History of changes to Unit

Version	Description of change	Date

Additional copies of this Unit specification can be purchased from the Scottish Qualifications Authority. Please contact the Business Development and Customer Support team, telephone 0303 333 0330.

General information for candidates

Unit title: Ethical Hacking Fundamentals

You will be introduced to the concepts and practical skills required in real life ethical hacking engagements.

By the end of this Unit you should be aware of the importance of the role of IT security and be able to perform information gathering steps, system security testing, system exploits, and access maintenance/track covering techniques and suggest possible countermeasures within a security assessment report.

On completion of the Unit you should be able to:

1 Perform target information gathering reconnaissance.
2 Perform system security vulnerability testing
3 Perform system vulnerability exploit attacks
4 Produce a security assessment report.

Ethical hacking is a wide area of research. There are a number of good resources listed here for training images, documentation, tutorials and links to other sites.

Consider joining an Open Web Application Security Project (OWASP) chapter. There are often useful resources and talks given on a regular basis, you may also find more information about open source projects that you can contribute to in some way.

As well as these resources you may wish to consider the following books:

Counter Hack Reloaded: A step by step guide to computer attacks and effective defences (ISBN-13: 978-0-13-148104-6) Edward Skoudis (2006)

NMAP Network scanning: The official NMAP project guide to network discovery and security scanning (ISBN 978-0-9799587-1-7) Gordon Fyodor Lyon (2009)

The Web Application Hacker's Handbook: Discovering and Exploiting Security Flaws (ISBN: 978-0-470-17077-9) Dafydd Stuttard (2007)

Hacking For Dummies, 3rd Edition (ISBN: 978-0-470-55093-9), Kevin Beaver (January 2010)