National Unit specification

General information

Unit title: Ethical Hacking (SCQF level 5)

Unit code: H9HY 45

Superclass: CC

Publication date: July 2015

Source: Scottish Qualifications Authority

Version: 01

Unit purpose

The purpose of this Unit is to develop an awareness of the knowledge and skills used by ethical and malicious hackers.

A specific aim of this Unit is to enhance learners' awareness of the potential threats from malicious hackers to individuals and organisations, and how ethical hacking can help identify and mitigate these threats. Additionally, learners will understand the legislation and ethics of hacking.

On completion of this Unit, learners will gain knowledge of the current legislation relating to computer hacking, and how this relates to their professional practice. Learners will be able to distinguish between methods used by ethical and malicious hackers to compromise individuals' and organisations' computer systems, as well as applying these skills to identify vulnerabilities. Learners may progress to the *Ethical Hacking* Unit at SCQF level 6 or similar National Units.

This Unit is a mandatory Unit within the National Progression Award in Cyber Security at SCQF 5.

Outcomes

On successful completion of the Unit the learner will be able to:

1 Describe current tools and techniques used by ethical and malicious hackers to compromise computer systems.
2 Explain current legislation relating to computer crime and hacking.
3 Perform a routine penetration test on a computer system within a controlled environment.

National Unit specification: General information (cont)

Unit title: Ethical Hacking (SCQF level 5)

Credit points and level

1 National Unit credit at SCQF level 5: (6 SCQF credit points at SCQF level 5)

Recommended entry to the Unit

Entry is at the discretion of the centre, however it would be beneficial if learners have gained the basic digital literacy and an understanding of cyber security issues which may be evidenced by possession of the *Ethical Hacking* Unit at SCQF level 4 or *Cyber Security Fundamentals* Unit at SCQF level 4 or equivalent qualifications or experience.

It is recommended that learners sign an acceptable use policy before using ethical hacking tools.

Core Skills

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

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

Context for delivery

This Unit may be offered stand-alone or as part of the National Progression Award in Cyber Security. If offered as part of this Group Award, there may be opportunities to combine and integrate teaching and learning across Units. There may also be opportunities to combine Evidence Requirements and integrate assessments.

The Assessment Support Pack (ASP) for this Unit provides assessment and marking guidelines that exemplify the national standard for achievement. It is a valid, reliable and practicable assessment. Centres wishing to develop their own assessments should refer to the ASP to ensure a comparable standard. A list of existing ASPs is available to download from SQA's website **(http://www.sqa.org.uk/sqa/46233.2769.html)**.

Equality and inclusion

This Unit specification has been designed to ensure that there are no unnecessary barriers to learning or assessment. The individual needs of learners should be taken into account when planning learning experiences, selecting assessment methods or considering alternative evidence.

Further advice can be found on our website **www.sqa.org.uk/assessmentarrangements**.

National Unit specification: Statement of standards

Unit title: Ethical Hacking (SCQF level 5)

Acceptable performance in this Unit will be the satisfactory achievement of the standards set out in this part of the Unit specification. All sections of the statement of standards are mandatory and cannot be altered without reference to SQA.

Outcome 1

Describe current tools and techniques used by ethical and malicious hackers to compromise computer systems.

Performance Criteria

(a) Describe the phases of an ethical hack and a malicious cyber-attack.
(b) Describe different computer tools and techniques that could be used to compromise computer systems.
(c) Describe different social engineering tools and techniques that could be used to compromise computer systems.

Outcome 2

Explain current legislation relating to computer crime and hacking.

Performance Criteria

(a) Explain the contemporary legislation relating to computer crime.
(b) Explain the contemporary legislation relating to hacking.
(c) Explain the use of a simple framework for engaging in penetration testing activities that protects organisations and individuals from prosecution.
(d) Explain the use of a simple framework for engaging in penetration testing activities that protects organisations and individuals from loss of confidentiality, integrity and availability of computer systems.

Outcome 3

Perform a routine penetration test on a computer system within a controlled environment.

Performance Criteria

(a) Identify the scope of a routine penetration test on a computer system.
(b) Perform reconnaissance on a penetration test scenario's footprint.
(c) Perform scanning and enumeration on a penetration test.
(d) Perform vulnerability scanning on a penetration test.
(e) Identify the risks, threats and vulnerabilities that have been exposed by the penetration test.
(f) Communicate the results of the penetration test.
(g) Maintain professional and ethical standard throughout all phases of a penetration test.

National Unit specification: Statement of standards (cont)

Unit title: Ethical Hacking (SCQF level 5)

Evidence Requirements for this Unit

Assessors should use their professional judgement, subject knowledge and experience, and understanding of their learners to determine the most appropriate ways to generate evidence and the conditions and contexts in which they are used.

Evidence is required to demonstrate that learners have achieved all Outcomes and Performance Criteria. However, sampling may be used in certain circumstances (see below).

The evidence for this Unit may be written or oral or a combination of these. Evidence may be captured, stored and presented in a range of media (including audio and video) and formats (analogue and digital). Particular consideration should be given to digital formats and the use of multimedia.

Whenever possible, evidence should be a naturally occurring by-product of teaching and learning. However, it must be produced by the learner. Authentication must be used where this is uncertain.

Evidence is required for two types of competence: evidence of **cognitive competence** (knowledge and understanding) and **evidence of practical competence** (practical abilities).

The evidence of cognitive competence will relate to Outcome 1 (all Performance Criteria) and Outcome 2 (all Performance Criteria).

Evidence of cognitive competence may be sampled so long as the sample is unknown, and unpredictable, to the learner. Where sampling is used to assess the learner's knowledge and understanding, an appropriate pass mark should be set.

The evidence of practical competence will relate to Outcome 3 (all Performance Criteria). The evidence will be the communication of the results of at least **one** routine penetration test on a computer system within a controlled environment. **At least two** tools and methods should be used for each of Performance Criteria (b), (c) and (d) of Outcome 3 to gather a range of information. The communication (Performance Criterion (f)) is an end-product and can take any appropriate form, however it should demonstrate all associated Performance Criteria in Outcome 3.

The Guidelines on Approaches to Assessment (see the Support Notes section of this specification) provide specific examples of instruments of assessment.

National Unit Support Notes

Unit title: Ethical Hacking (SCQF level 5)

Unit Support Notes are offered as guidance and 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 will introduce learners who are considering a career in computing and Information Technology to the key concepts in hacking, and identifying the key difference between ethical and malicious hackers.

With increasingly open systems organisations and individuals are faced with a range of threat factors. This Unit will introduce the nature of a range of risks, threats and vulnerabilities that open IT systems are exposed to, considering infrastructure security and application security.

The focus of this Unit is **ethical** hacking and **all learning and teaching must be delivered in that context**. It is vital that learners appreciate the distinction between ethical and malicious hacking. Learner activities must also be carried out in that context. Ethics must be emphasised throughout this Unit **in every Outcome**. Learners must be made aware of the consequences of malicious hacking, and recognise their responsibilities when they carry out practical activities.

Given the ubiquity of computer networks, their operational principles should be known and understood, and the potential attacks and defences in a networked environment should be discussed.

Outcome 1 will provide learners with knowledge of common phases of a malicious attack and penetration test and typical contemporary tools and techniques used in these five phases:

1 Reconnaissance
2 Scanning and Enumeration
3 Exploitation
4 Post-Exploitation
5 Covering Tracks

Outcome 2 will provide learners with a grounding in the legislation covering important factors which determine ethical and legal use of computing equipment. The importance of maintaining confidentiality, integrity and security during a penetration test will provide the background to define the difference between ethical and unethical, legal and illegal activities.

National Unit Support Notes (cont)

Unit title: Ethical Hacking (SCQF level 5)

The following Scottish and UK legislation is not exhaustive, but at the time of writing the following legislation should be considered:

- Data Protection Act (1998)
- Computer Misuse Act (1990)
- Copyright, Design and Patents Act (1988)
- Intellectual Property Act (2014)
- Regulation of Investigatory Powers Act (2000)
- Police and Justice Act (2006)

Outcome 3 will provide learners an opportunity to learn about using some basic tools and techniques for reconnaissance, scanning and enumeration as part of a penetration test. This should include 'passive' information gathering using public information and the use of some simple tools that allow learners to create a profile of an organisation and potential vulnerabilities. Emphasis should be placed on agreeing and sticking to an agreed penetration test scope and the importance of maintaining professional standards.

Guidance on approaches to delivery of this Unit

A practical hands-on approach to learning should be adopted to engage learners and exemplify key concepts. However, all practical activities should be underpinned with appropriate knowledge before learners commence these activities.

It is recommended that learners gain hands-on experience of applying as many basic current methods used to footprint, scan and enumerate computer infrastructure and applications in a controlled environment as possible. Learners should be reminded at all times to adhere to the law and not use any skills learnt without an appropriate penetration test agreement and the permissions applicable to the scope of that agreement. It is recommended that an agreement with a 'live partner' is formed to provide meaningful reconnaissance activities using tools to examine publically available information on social media, company records, DNS registrations, company websites and other similar publically available information. It must be stressed to learners about using skills learnt from this Unit responsibly. **The use of sandboxed virtualised environment support platforms such as Kali Linux and scenarios such as those provided by Rapid7 and OWASP is strongly recommended.**

The actual distribution of time between Outcomes is at the discretion of the centre. However, one possible approach is to distribute the available time as follows, with emphasis on the practical tasks:

- Outcome 1: 8 hours
- Outcome 2: 10 hours
- Outcome 3: 22 hours

National Unit Support Notes (cont)

Unit title: Ethical Hacking (SCQF level 5)

Guidance on approaches to assessment of this Unit

Evidence can be generated using different types of assessment. The following are suggestions only. There may be other methods that would be more suitable to candidates.

Centres are reminded that prior verification of centre-devised assessments would help to ensure that the national standard is being met. Where candidates experience a range of assessment methods, this helps them to develop different skills that should be transferable to work or further and higher education.

The Outcomes can be assessed in a variety of ways. A traditional approach would involve the testing of knowledge in Outcomes 1 and 2 through a selected response instrument (such as a multiple choice test). There is no requirement for all legislation in Outcome 2 to be assessed in every test. The sample should be sufficiently random and robust to clearly infer competence in the whole knowledge domain. Every Performance Criterion must be covered in the test; the relative weighting of each one is left to the discretion of the assessor. An appropriate pass mark must be set. The pass mark will be influenced by the instrument of assessment. All of the associated Performance Criteria must be satisfied. It is recommended that if this approach is adopted then all of the knowledge and understanding in this Unit is combined into a single test that samples from the knowledge domain, with an appropriate pass mark. For example, multiple-choice test, comprising 25 questions, each with four options (A–D), could have a pass mark of 15.

The remaining practical competencies in Outcome 3 could be assessed as part of a case study which is a simulation of a penetration test for a fictional organisation. Candidates should be provided with examples of footprint information that would typically be available from Open Source Intelligence, public information sources such as Company Registers, Domain Registrars, social media and company websites and other relevant publically available information. Candidates should use the footprint information to perform the necessary penetration tests on a sandboxed computer system as required by Performance Criteria (b-d) with some common contemporary vulnerabilities which sampled the knowledge domain. As part of the simulation the candidate would need to agree a scope and produce a simple penetration report. The report should summarise the organisation's footprint and identify key information such as hosts, ports, operating systems, applications and known vulnerabilities of the computer system under test.

Another approach to assessment would be the creation and maintenance of a log or blog, which would record candidate activity throughout the Unit. The activity log would record all of the learning and practical activities carried out by the candidate for a Case Study. The completed log must satisfy all of the Performance Criteria in all of the Outcomes. For example, the journal entry/entries relating to Outcome 2, Performance Criterion (a) and (b), would have to identify appropriate current legislation for Scottish and UK laws relating to computer crime and hacking. Sampling is not appropriate when this approach is used. While all of the Performance Criteria must be satisfied, the evidence may be distributed across the entire journal. It is not necessary for a specific Performance Criterion to be satisfied entirely within a specific journal entry. Professional judgement should be exercised when a Performance Criterion is evidenced across several entries.

Given that the journal will be completed over an extended period of time, perhaps in a number of locations, the completed log must be authenticated. Authentication may take various forms including, but not limited to, oral questioning and plagiarism checks. A statement of authenticity should be provided by the candidate to verify the work as their own, and also state any necessary sources and permissions (if any). Practical activities could also be recorded via the blog. When practical activity is recorded on a blog (narratively), authentication could involve a photograph or video of candidate activity (this could be included as part of their post). Not every practical task would require authentication; at this level it is acceptable for some posts to be a simple description of appropriate practical activities.

The critical aspect is that the blog and simulation are an overall accurate reflection of the practical activities (and, therefore, the associated skills) carried out by the candidate during the life of the Unit.

Another approach would involve the creation and maintenance of an e-portfolio. The e-portfolio would include all of the statements, identifications, descriptions and selections necessary to satisfy the criteria relating to cognitive competencies, together with digital artefacts that provide evidence of their practical abilities. Digital artefacts would include screenshots, digital photographs, audio and video recordings, etc that collectively evidence candidates' competencies. Some form of authentication would be required. This could be as simple as a statement of originality, signed by the candidate and the assessor.

Opportunities for 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 learner evidence and that conditions of assessment as specified in the Evidence Requirements are met, regardless of the mode of gathering evidence. The most up-to-date guidance on the use of e-assessment to support SQA's qualifications is available at **www.sqa.org.uk/e-assessment**.

Opportunities for developing Core and other essential skills

This Unit provides opportunities to develop some of the following Core Skills:

Communication (SCQF level 5)
Numeracy (SCQF level 5)
Information and Communication Technology (SCQF level 5)
Problem Solving (SCQF level 5)

Some of the Core Skill components in *Communication* can be developed within this Unit. Learners are required to evaluate a range of written communication and perform actions dependent upon the information contained. Learners are also required to produce written communication to present essential information which adheres to a required format. There are opportunities to develop the use of spelling, grammar and punctuation to convey the essential information.

National Unit Support Notes (cont)

Unit title: Ethical Hacking (SCQF level 5)

Some of the Core Skill components in *Numeracy* can be developed within this Unit. Learners can develop their skills in interpreting and presenting graphical information in the form of network diagrams and other graphical data. Learners will also have an opportunity to develop Number skills working with numerical information such as Internet Protocol addresses and Port numbers.

Some of the Core Skill components in *ICT* can be developed within this Unit. Learners will need to select and launch appropriate applications to perform a range of tasks. Learners will also need to search for a range of information and select appropriate sources. Learners will need to evaluate, integrate and present information in an appropriate format.

Some of the Core Skill components in *Problem Solving* can be developed within this Unit. Learners will need to make choices on how best to proceed with a familiar task given a novel set of data. As part of their tasks Learners will need to decide on which approach to take and organise that approach taking the correct steps to improve their efficiency.

History of changes to Unit

Version	Description of change	Date

General information for learners

Unit title: Ethical Hacking (SCQF level 5)

This section will help you decide whether this is the Unit for you by explaining what the Unit is about, what you should know or be able to do before you start, what you will need to do during the Unit and opportunities for further learning and employment.

The purpose of this Unit is to introduce those who are considering specialising in Computing and IT related disciplines to the principles behind ethical hacking and the challenges faced by individuals and organisations.

Individuals, Organisations and Nations are increasingly open and rely on highly integrated computer systems and infrastructure. This openness and level of integration introduces risks and vulnerabilities providing opportunities for threats to compromise systems for a range of malicious purposes including identity theft, fraud, theft, espionage, terrorism and other forms of cybercrime.

This Unit will introduce a range of the Open Source Intelligence and other direct forms of intelligence gathering techniques and tools used by ethical and malicious hackers to compromise systems. The Unit introduces the legal and moral frameworks that exist and define the difference between the legal, ethical hacker — the white hat, and the illegal, malicious hacker — the black hat. The core principles of Confidentiality, Integrity and Availability of computer systems, and the importance of these, will also be introduced.

Learners will explore how to conduct a routine penetration test to a computer system as an ethical hacker within a controlled environment to identify and report on the footprint and vulnerabilities of a computer system and how this information can be used to better protect individuals and organisations.

The assessment may take different forms. It may involve a short test of your knowledge and some practical tasks, or be assessed as part of a case study which is a simulation of a penetration test for a fictional organisation. You will need to produce a simple penetration report on the risks, threats and vulnerabilities a computer system is exposed to, identified by the penetration test.

This Unit may be studied by itself or as part of the National Progression Award in Cyber Security at SCQF level 5. Learners may also progress onto the *Ethical Hacking* Unit at SCQF level 6.