National Unit specification

General information

Unit title: Ethical Hacking (SCQF level 6)

Unit code: H9HY 46

Superclass: CC

Publication date: July 2015

Source: Scottish Qualifications Authority

Version: 01

Unit purpose

The purpose of this Unit is to develop a detailed understanding of tools and techniques used by ethical and malicious hackers.

A specific aim of this Unit is to provide learners with an understanding of the potential threats, factors and tools that can be leveraged by malicious hackers to target individuals and organisations. Learners will demonstrate an understanding of how ethical hacking can help identify and mitigate these threats. Learners will also be introduced to some of the techniques and technologies used to defend systems from attack. Additionally, learners will evaluate the legislation and ethics of hacking.

On completion of this Unit, learners will be able to explain and apply the main methods used by malicious hackers to compromise individuals' and organisations' systems in a controlled environment. They will be able to identify, explain and suggest remediation for common vulnerabilities as well being able to make informed choices about the ethics of hacking based on an understanding of current legislation. Learners may progress to National Certificates or Higher National Certificates in Computing or related qualifications.

This Unit is a mandatory Unit within the National Progression Award in Cyber Security at SCQF 6.

Outcomes

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

1 Analyse current trends in cybercrime.
2 Evaluate contemporary legislation relating to cybercrime.
3 Perform a complex penetration test on a computer system in a controlled environment.

National Unit specification: General information (cont)

Unit title: Ethical Hacking (SCQF level 6)

Credit points and level

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

Recommended entry to the Unit

Entry is at the discretion of the centre. However, it is recommended that learners have some prior knowledge in Computing or IT systems. It would be beneficial if learners possess digital literacy skills and an understanding of cyber security issues, which may be evidenced by possession of the *Ethical Hacking* Unit at SCQF level 5 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 at SCQF level 6. 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 6)

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

Analyse current trends in cybercrime.

Performance Criteria

(a) Describe real life historical and contemporary examples of cybercrime.
(b) Compare historical and contemporary threats in cybercrime.
(c) Compare historical and contemporary techniques deployed by malicious individuals, groups and nations.
(d) Explain changes in professional and ethical approaches in relation to cybercrime.

Outcome 2

Evaluate contemporary legislation relating to cybercrime.

Performance Criteria

(a) Describe contemporary legislation relating to cybercrime.
(b) Critique contemporary legislation relating to computer crime.
(c) Identify potential omissions in current legislation relating to cybercrime.
(d) Identify potential ethical threat caused by current legislation including threats to personal privacy and political freedom.
(e) Use legal and technical terminology relating to cybercrime correctly.

Outcome 3

Perform a complex penetration test on a computer system in a controlled environment.

Performance Criteria

(a) Scope a given system or web based penetration test.
(b) Conduct target information gathering reconnaissance.
(c) Use a range of hacking tools and techniques to demonstrate system or web based security vulnerability testing.
(d) Conduct system or web based vulnerability exploit attacks.
(e) Identify the risks, threats and vulnerabilities exposed by a penetration test, and how an attacker may leverage them.
(f) Communicate the results of the penetration test including basic remediation procedures.
(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 6)

Evidence Requirements for this Unit

Assessors should use their professional judgement, subject knowledge, 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. Sampling may be used in certain circumstances (see below) where the sample is sufficiently random and robust to clearly infer competence in the complete domain.

The evidence for this Unit may be written, 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: **cognitive competence** (knowledge and understanding) and **practical competence** (practical abilities).

Evidence of cognitive competence may be sampled across the knowledge domain defined by this Unit Specification, 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 cognitive competence will relate to Outcome 1 (all Performance Criteria) and Outcome 2 (all Performance Criteria). Where this evidence is not sampled, the scope of the evidence should be limited to the most common trends (Outcome 1) and most relevant legislation (Outcome 2). If sampling is used, the evidence must be produced under controlled conditions with the sample unknown and with no access to reference material.

The evidence of practical competence will relate to Outcome 3 (all Performance Criteria). The evidence will be the communication of the results including basic remediation procedures of **at least one complex penetration test** on **at least one computer system** within a controlled environment. **At least three tools and techniques** should be used for Performance Criterion (c). 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) provides specific examples of instruments of assessment.

National Unit Support Notes

Unit title: Ethical Hacking (SCQF level 6)

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

The purpose of this Unit is to equip learners with theoretical and hands on knowledge about cyber security. As such they will be required to demonstrate practical skills.

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 is knowledge based. It requires an understanding of the main historical and contemporary threats in cybercrime and techniques used. Resources are listed in the next section to help identify these common threats and attacks. As mentioned in the Evidence Requirements for this Outcome demonstration of understanding attacks can take many forms and in this particular case may not need to be practical. However, it could serve as a good introduction to the technologies used in the further Outcomes. Cybercrime changes on an almost weekly basis, new attacks are discovered, old attacks are adapted, previously relied on technologies are found to have major flaws. Therefore in Outcome 1 learners are expected, not to become experts, but to have a general understanding of the motives of the individuals and groups involved and the types of attacks they favour. Learners should be able to demonstrate knowledge of some of the more recent vulnerabilities.

Outcome 2 is based on legal considerations. 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)

National Unit Support Notes (cont)

Unit title: Ethical Hacking (SCQF level 6)

Outcome 3 requires that learners demonstrate practical skills in attacking and defending systems. This must be achieved in a controlled environment. Advice about achieving the proper level of control is given in the Approaches to Delivery of this Unit section.

In short, learners should adopt a standard penetration testing structure to achieve this. This structure is as follows:

- Agreeing the Scope of the test
- Reconnaissance and (if appropriate OSINT — Open Source Intelligence Gathering)
- Scanning and enumeration of services
- Manual penetration testing, vulnerability research and scoring
- Exploitation (with prior approval once a vulnerability has been identified — this may be oral permission)

The three other stages of security testing are Post-Exploitation (retrieving information), maintaining access and covering your tracks. It is important that learners know the existence of these stages. However, due to the sensitive nature and the legal implications, it is not advised that these areas be explicitly taught as practical activities. Learners should work to one on the many penetration testing frameworks available, for example learners doing web assessments should use the OWASP Top 10.

Guidance on approaches to delivery of this Unit

This Unit requires a level of technical and theoretical knowledge to be demonstrated. It is recommended that as each new concept is introduced learners are given theoretical grounding before practical activities commence. As such it is STRONGLY suggested that learned sign an acceptable use policy before commencing the course.

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

In order for learners to experience the use of these tools a controlled environment must be set up. Learners should be encouraged to experiment with a variety of tools within the environment as in reality many tools are deployed to achieve the same aim. A convenient way to do this would be to run a Linux security distribution on dedicated machines such as a Raspberry Pi or an older repurposed computer. Likewise vulnerable websites and servers may be similarly arranged so all malicious traffic is kept to a contained network. Advice on how to set up such contained systems may be found in the resources document.

While learners will be required to demonstrate their own mastery of the skills, there are opportunities for paired work. In fact, studies show that paired coding/paired hacking is a very effective educational experience.

National Unit Support Notes (cont)

Unit title: Ethical Hacking (SCQF level 6)

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 learners.

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

Outcome 1 requires knowledge and understanding of the current trends in cybercrime to be demonstrated. The evidence for Outcome 1 may take the form of a written test/report or presentation or other oral evidence that shows the candidate satisfies all of the associated Performance Criteria. There is no requirement for the Performance Criterion (c) to be demonstrated practically.

Outcome 2 is focussed on legal issues. The evidence for Outcome 2 may take the form of a written test that shows the candidate satisfies all of the associated Performance Criteria. There is no requirement for all pieces of legislation (Outcome 2) to be assessed in every test. The written test should be taken under closed-book conditions. The sample must be sufficient 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.

Outcome 3 requires practical skills to be demonstrated and an accompanying checklist may be provided in order to assure authenticity.

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. 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.

National Unit Support Notes (cont)

Unit title: Ethical Hacking (SCQF level 6)

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**.

National Unit Support Notes (cont)

Unit title: Ethical Hacking (SCQF level 6)

Opportunities for developing Core and other essential skills

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

Communication (SCQF level 6)
Numeracy (SCQF level 6)
Information and Communication Technology (SCQF level 6)
Problem Solving (SCQF level 6)

Some of the Core Skill components in *Communication* can be developed within this Unit. Learners are required present their findings in either written or oral format. Learners are also required to produce written communication of their finding with fits a standard reporting format. There are opportunities to develop the use of spelling, grammar and punctuation to convey the essential information.

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 6)

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.

This Unit is designed for learners who wish to peruse an interest in IT, Computing and in particular Computer Security. It will equip you with an understanding of the cyber threats which modern companies and individuals face.

In this Unit, you will be taught the basics of Ethical Hacking as a methodology to assess the security position of a given system, web based or infrastructure based. You will learn how malicious attackers gain information about systems through passive means and by using Open Source Intelligence (website, social media, etc). You will learn how to scan and map a given system, identify common vulnerabilities and use basic exploits in a controlled environment. You will then learn to present your findings and suggestions on basic fixes for commonly identified problems.

The assessment may take different forms. It may involve a short test of your knowledge and some practical tasks. You may be required to produce a penetration report on the risks, threats and vulnerabilities a computer system is exposed to, identified by the penetration test and suggest some basic remediation procedures.

This Unit may be studied by itself or as part of the National Progression Award in Cyber Security at SCQF level 6. Learners may progress to National Certificates or Higher National Certificates in Computing or related qualifications.