Higher National Unit Specification

General information

Unit title: Ethical Hacking (SCQF level 7)

Unit code: J0HK 34

Superclass: CC

Publication date: August 2018

Source: Scottish Qualifications Authority

Version: 02

Unit purpose

The purpose of this unit is to provide learners with an understanding of the threats, factors and tools that can be leveraged by malicious hackers to target individuals and organisations. During this unit, learners will learn the techniques and technologies used to defend systems from attack and evaluate the legislation and ethics of hacking.

This is a **non-specialist** unit, intended for learners with an interest in cyber security. It is particularly suitable for learners who are undertaking an HN in Cyber Security, Computer Science or Computing Networking.

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 also be able to identify, explain and implement remediation for common vulnerabilities.

At the completion of this unit, learners may progress to J0HB 34 *Penetration Testing* at SCQF level 7.

Outcomes

On successful completion of the unit, the learner will be able to:

1 Explain ethical hacking.
2 Plan a penetration test.
3 Use current techniques to undertake a penetration test and exploit system vulnerability.
4 Implement appropriate countermeasures to mitigate a cyber-attack.

Higher National Unit Specification: General information (cont)

Unit title: Ethical Hacking (SCQF level 7)

Credit points and level

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

Recommended entry to the unit

No previous knowledge or experience is required and access to this unit will be at the discretion of the centre. However, it would be beneficial if learners had some prior knowledge and skills in computing/information technology/networking. This may be evidenced by possession of relevant National Units, such as the *Ethical Hacking* units at SCQF level 4, 5 or 6.

Core Skills

Achievement of this Unit gives automatic certification of the following Core Skills component:

Complete Core Skill Problem Solving at SCQF level 6

Core Skill component Assessing Information at SCQF level 5

There are also opportunities to develop aspects of Core Skills which are highlighted in the Support Notes of this Unit specification.

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.

This unit may be delivered in conjunction with J0HB 34 *Penetration Testing*.

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**.

Higher National Unit Specification: Statement of standards

Unit title: Ethical Hacking (SCQF level 7)

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.

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. Learners 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

Explain ethical hacking.

Knowledge and/or skills

- Definition of ethical hacking
- Benefits of ethical hacking
- Process behind hacking attacks
- Threats, factors, tools and techniques
- Cybercrime
- Contemporary legislation
- Professionalism, legislation and ethics of ethical hacking

Outcome 2

Plan a penetration test.

Knowledge and/or skills

- Rules of engagement
- Reconnaissance
- Enumeration
- Maintaining access
- Covering tracks

Outcome 3

Use current techniques to undertake a penetration test and exploit system vulnerability.

Knowledge and/or skills

- Manual vulnerability testing
- Automatic vulnerability testing
- Documentation of processes

Higher National Unit Specification: Statement of standards (cont)

Unit title: Ethical Hacking (SCQF level 7)

Outcome 4

Implement appropriate countermeasures to mitigate a cyber-attack.

Knowledge and/or skills

- Identification of appropriate countermeasures
- Implementation of countermeasures
- Testing of countermeasures
- Mitigation procedures
- Communication to target audience

Evidence requirements for this unit

Learners will need to provide evidence to demonstrate the knowledge and/or skills across all outcomes. The evidence requirements for this unit will take three forms.

1 Knowledge evidence (All outcomes)
2 Product evidence (Outcomes 2, 3 and 4)
3 Performance evidence (Outcomes 2, 3 and 4)

The **knowledge evidence** will comprise the underpinning knowledge required in Outcomes 1, 2, 3 and 4. Evidence is normally required for all knowledge and/or skills statements except those explicitly relating to skills. The knowledge evidence may be sampled when testing is used.

The knowledge evidence may be sampled when testing is used. In this case, the evidence must be produced under controlled conditions in terms of location (supervised), timing (limited) and access to reference materials (not permitted). The sampling frame must cover all outcomes but not all knowledge/skills statements; however, the majority of the knowledge/skills should be sampled in every test. The sampling frame must always include the following:

- Benefits of ethical hacking and why it is required
- Processes behind hacking attacks leading to what are the threats, factors, tools and techniques used
- Legal and ethical aspects of working in the ethical hacking/penetration, including cybercrime and the relevant legislation
- An understanding of how to create a 'rules of engagement' document and the importance and implications should this not be followed
- The five areas of a penetration test, including:
  - rules of engagement and why they are required
  - definition of reconnaissance and what tools and techniques can be used
  - definition of enumeration
  - maintaining access to a system
  - techniques that might be used by a hacker to cover their tracks and prevent detection
- Types of penetration test that can be carried out and what form these take
- Types of countermeasures that may be used to protect systems from attack

The knowledge evidence 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).

The **product evidence** will relate to Outcomes 2, 3 and 4. It will demonstrate that the learner is able to plan and carry out a penetration test to exploit vulnerabilities of a system, in a real or simulated environment. The learner is also required to identify and implement appropriate countermeasures to prevent a hacker from being able to exploit the vulnerabilities found. All the steps taken during reconnaissance and testing must be documented. The results of the penetration test, including mitigation procedures, should be recorded and communicated to a target audience.

This evidence may be produced over the life of the unit, under loosely controlled conditions (including access to reference materials). Authentication will be necessary (see below).

The **performance evidence** for Outcomes 2, 3 and 4 will demonstrate correct procedures are being followed from setting rules of engagement, to reconnaissance, to finding vulnerabilities, exploiting them and identifying and implementing appropriate countermeasures.

The SCQF level of this unit (level 7) provides additional context on the nature of the required evidence and the associated standards. The following level descriptors are particularly relevant to the evidence.

- An overall appreciation of the body of knowledge
- Knowledge that is embedded in the main theories, concepts and principles
- Apply knowledge and skills in practical contexts
- Use some of the basic and routine professional skills, techniques, practices and materials
- Use a range of approaches to address defined and/or routine problems
- Exercise some initiative and independence in carrying out defined activities at a professional level
- Take account of own and others' roles and responsibilities when carrying out tasks

These level descriptors should be used (explicitly or implicitly) when making judgements about the evidence.

When evidence is produced in uncontrolled or loosely controlled conditions, it must be authenticated. The Guide to Assessment provides further advice on methods of authentication.

The support notes section of this specification provides specific examples of instruments of assessment that will generate the required evidence.

Higher National Unit Support Notes

Unit title: Ethical Hacking (SCQF level 7)

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 is designed to give learners an opportunity to learn about the role of ethical hacking.

Learners should learn that ethical hacking is a vital part of computing. Operating systems, applications, network infrastructure components, physical security and business processes must be tested in order to ensure 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.

Please note that the following guidance, relating to specific outcomes, does not seek to explain each knowledge/skills statement, which is left to the professionalism of the teacher. It seeks to clarify the statement of standards where it is potentially ambiguous. It also focuses on non-apparent teaching and learning issues that may be over-looked, or not emphasised, during unit delivery. As such, it is not representative of the relative importance of each knowledge/skill.

Outcome 1: Explain ethical hacking.

This outcome relates to the majority of the underpinning knowledge required for the unit. It should be made clear to the learner the professionalism and ethics required when performing a penetration test, stressing the importance of clear rules of engagement when planning a penetration test.

Cybercrime and the process behind attacks could use contemporary news reports as a background, it is likely that that the learner may be familiar with these. This should then lead on to the tools and techniques that might have been used to carry out those attacks.

Benefits of being a Certified Ethical Hacker, job roles, rewards, national shortage should be explored when delivering Outcome 1.

Higher National Unit Support Notes (cont)

Unit title: Ethical Hacking (SCQF level 7)

Outcome 2: Plan a penetration test.

This outcome should cover the phases in planning a penetration test and should give learners a chance to learn these skills. This process should begin with the importance of defining the scope of the test, by agreeing a set of rules of engagement. This should also lead into professional qualifications in ethical hacking and how these can ensure professionalism.

Once the footprint has been agreed, then a number of reconnaissance techniques should be discussed, such as port scanning, identifying active machines. This phase may also lead into social engineering.

Enumeration is the first attack that takes place on target network and is the process that is used to gather information about a target machine by actively connecting to it. By using enumeration, an ethical hacker will be looking to identify the user, system and admin account information, perhaps by enumerating windows active directory. This should include how a learner might establish an active connection to the target hosts to discover potential attack vectors in the system.

Once the initial enumeration attack has taken place, then maintaining access to the system should become a priority, this might be by adding a new user account, changing a user password or by adding some sort of Trojan that will allow future access.

Once these steps have been carried out, the hacker can then cover their tracks by removing evidence of intrusion.

Outcome 3: Use current techniques to undertake a penetration test and exploit system vulnerability.

This outcome should be delivered through a practical task based on the knowledge gained in Outcome 2. Learners could be given a vulnerable client system to carry out a penetration test on.

Outcome 4: Implement appropriate countermeasures to a cyber-attack.

A range of countermeasure should be explored in this outcome, whether it be patching of operating systems, use of intrusion detection or intrusion protection systems. The learner should have a clear understanding of how countermeasures can be selected and used.

Guidance on approaches to delivery of this unit

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 learners are given as many opportunities as possible to learn from practical experiences. The Certified Ethical Hacker qualification is the current industry leading qualification and there a number of useful online resources available.

Higher National Unit Support Notes (cont)

Unit title: Ethical Hacking (SCQF level 7)

There are a number of useful resources already available online and could 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/metasploitunleashed/Metasploit_Unleashed_Information_Security_Training — Online manual for metasploit.

A suggested distribution of time, across the outcomes, is:

Outcome 1: 10 hours
Outcome 2: 10 hours
Outcome 3: 10 hours
Outcome 4: 10 hours

Summative assessment may be carried out at any time. However, when testing is used (see evidence requirements) it is recommended that this is carried out towards the end of the unit (but with sufficient time for remediation and re-assessment). When continuous assessment is used (such as the use of a web log), this could commence early in the life of the unit and be carried out throughout the duration of the unit.

There are opportunities to carry out formative assessment at various stages in the unit. For example, formative assessment could be carried out on the completion of each outcome to ensure that learners have grasped the knowledge contained within it. This would provide educators with an opportunity to diagnose misconceptions, and intervene to remedy them before progressing to the next outcome.

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.

Higher National Unit Support Notes (cont)

Unit title: Ethical Hacking (SCQF level 7)

The **knowledge evidence** required comprises the underpinning knowledge required in Outcomes 1, 2, 3 and 4. A test may comprise:

1 A selected response test consisting of four options (one key) with a pass mark of 60%.The test could consist of a relatively high number of questions (30 or 40 for example), lasting an hour, which would span all of the outcomes and sample all of the knowledge statements (including at least one question for each statement).

Or

2 A constructed response test comprising a number of short answer questions, marked and assessed traditionally. For example, the test may comprise of 10 questions, requiring a response of no more than one or two paragraphs. Questions would be selected across all three outcome and would each be worth five marks. Learner responses would be marked out of 50 with a pass mark of 25. If this approach is taken, it is recommended that some (or all) of the questions combine the knowledge and understanding within and across outcomes. This test would be taken, sight-unseen, in controlled and timed conditions without reference to teaching materials. A suitable duration would be 60 minutes.

Or

3 A more contemporary approach to assessment would involve the use of a web log (blog) to record learning (and the associated activities) throughout the life of the unit. The blog would provide knowledge evidence (in the descriptions and explanations) and product evidence (using, for example, video recordings). The blog should be assessed using defined criteria to permit a correct judgement about the quality of the digital evidence. In this scenario, every knowledge and skill must be evidenced; sampling would not be appropriate.

The **product evidence** will relate to Outcomes 2, 3 and 4. It will demonstrate that the learner is able to plan and carry out a penetration test to exploit vulnerabilities of a system, in a real or simulated environment. The learner is also required to identify and implement appropriate countermeasures to prevent a hacker from being able to exploit the vulnerabilities found. All the steps taken during reconnaissance and testing must be documented. The results of the penetration test, including mitigation procedures, should be recorded and communicated to a target audience.

The product evidence may be evidenced by a video or screen capture showing that all steps required have been carried out. This can be annotated or provided with a voiceover describing the steps taken.

The **performance evidence** for Outcomes 2, 3 and 4 will demonstrate that correct procedures are being followed, from setting rules of engagement to reconnaissance, to finding vulnerabilities, exploiting them and identifying and implementing appropriate countermeasures.

The product and performance evidence may be evidenced together by a report that covers the evidence requirements for Outcomes 2, 3 and 4.

Higher National Unit Support Notes (cont)

Unit title: Ethical Hacking (SCQF level 7)

This evidence may be produced over the life of the unit, under loosely controlled conditions (including access to reference materials). Authentication will be necessary (see below).

There could be opportunities to cross-assess outcomes or parts of outcomes within this unit with other units where similar or subject-related evidence is retained. This would be appropriate and acceptable when centres wish to avoid duplication for learners, to increase efficiency for all, and to cut down on the assessment load for learners.

The evidence should be generated under supervised conditions and work can be authenticated by continual observation or by individual questioning to ensure that it is the learner's own work.

Formative assessment could be used to assess learners' knowledge at various stages throughout the life of the unit. An ideal time to gauge their knowledge would be at the end of each outcome. This assessment could be delivered through an item bank of selected response questions, providing diagnostic feedback to learners (when appropriate).

If a blog is used for summative assessment, it would also facilitate formative assessment since learning (including misconceptions) would be apparent from the blog, and intervention could take place to correct misunderstandings on an on-going basis.

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

The Core Skill of *Working with Others* may be evidenced during the phases of the test that involve setting rules of engagement and providing mitigations.

This Unit has the Core Skill of Problem Solving embedded in it, so when learners achieve this Unit their Core Skills profile will be updated to show that they have achieved Problem Solving at SCQF level 6

This Unit has the Assessing Information component of Information and Communication Technology embedded in it. This means that when learners achieve the Unit, their Core Skills profile will also be updated to show they have achieved Assessing Information at SCQF level 5.

History of changes to unit

Version	Description of change	Date
02	Core Skill Problem Solving at SCQF level 6 embedded. Core Skill Component Assessing Information at SCQF level 5 embedded	31/08/18

General information for learners

Unit title: Ethical Hacking (SCQF level 7)

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 will provide you with an introduction to ethical hacking. You will gain an understanding of the threats, factors and tools that can be used by malicious hackers to target individuals and organisations. The aim of the unit is, that by knowing the tools that malicious hackers use, you will then learn the techniques and technologies used to defend systems from attack and, in doing so, evaluate the legislation and ethics of hacking.

On completion of this unit, you will be able to explain and apply the main methods used by malicious hackers to compromise individuals and organisations' systems in a controlled environment. You will also be able to identify, explain and implement remediation for common vulnerabilities.

On successful completion of the unit, you will be able to:

- Explain ethical hacking.
- Plan a penetration test.
- Use current techniques to undertake a penetration test and exploit system vulnerability.
- Implement appropriate countermeasures to mitigate a cyber-attack.

You will be assessed using a number of methods, which will test your knowledge and practical skills. This could be by questioning or by producing a report based on a penetration test that you have carried out.

This Unit has the Core Skill of Problem Solving embedded in it, so when you achieve this Unit your Core Skills profile will be updated to show that you have achieved Problem Solving at SCQF level 6.

This Unit has the Assessing Information component of Information and Communication Technology embedded in it. This means that when you achieve the Unit, your Core Skills profile will also be updated to show you have achieved Assessing Information at SCQF level 5.