# Higher National Unit Specification

## General information

**Unit title:** Penetration Testing (SCQF level 7)

**Unit code:** J0HB 34

**Superclass:** CC

**Publication date:** August 2018

**Source:** Scottish Qualifications Authority

**Version:** 02

## Unit purpose

The purpose of this unit is to introduce learners to the principles and practice of penetration testing. The units looks at authorised simulated attacks on computer systems, which explore security weaknesses that may potentially provide access to the systems' features and data.

It is a **non-specialist unit**, intended for a wide range of learners; it is particularly appropriate for learners with an interest in computing and its associated sub-disciplines, including cyber security.

The unit covers the underlying principles of penetration testing, identifying weaknesses and strengths within a given system. It examines how penetration tests interact with ethical hacking and legal issues. It stresses the importance of working with the client and using analysis techniques, such as flaw hypothesis methodology, to identify and prioritise potential flaws. Dependent on the system involved in the test, it covers use of appropriate testing tools and techniques, and designing tests on programs, servers, web applications, network infrastructure or mobile applications. It covers the documentation of these test results and evaluation of these as part of a security audit.

On completion of this unit, learners will understand the concepts underpinning penetration testing. Learners may progress onto other cyber security units at SCQF level 7 or higher.

## Higher National Unit Specification: General information (cont)

## Unit title: Penetration Testing (SCQF level 7)

## Outcomes

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

1 Describe the concepts underpinning penetration testing.
2 Design a penetration test from a given scenario.
3 Implement a penetration test from a given scenario.
4 Evaluate a penetration test as part of a test audit.

## 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 in this unit. However, if it is delivered as part of a Higher National award, then previous knowledge of that area would be beneficial. For example, if this unit is delivered as part of Cyber Security, Software Development or Web Development, then knowledge of an appropriate scripting language would be beneficial.

## Core Skills

Achievement of this Unit gives automatic certification of the following:

Complete Core Skill Problem Solving at SCQF level 5

Core Skill component None

Opportunities to develop aspects of Core Skills are highlighted in the Support Notes for 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 J0HK 34 *Ethical Hacking*.

## 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: Penetration Testing (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

Describe the concepts underpinning penetration testing.

### Knowledge and/or skills

- Definition of cyber security and cyber resilience
- Penetration testing, ethical hacking and legal issues
- Tools and techniques of penetration testing
- Network security policies
- Stages in a penetration test
- Types of penetration testing and testers
- Penetration testing processes
- Penetration testing reporting

## Outcome 2

Design a penetration test from a given scenario.

### Knowledge and/or skills

- Test planning steps
- Information analysis/intelligence gathering
- Identification of vulnerabilities (manual/automatic tools)
- Identification of risks
- Test methodologies
- Test designs

## Outcome 3

Implement a penetration test from a given scenario.

### Knowledge and/or skills

- Implementation of penetration test (intrusion attempts)
- Documentation of penetration test

## Higher National Unit Specification: Statement of standards (cont)

## Unit title: Penetration Testing (SCQF level 7)

## Outcome 4

Evaluate a penetration test as part of a test audit.

### Knowledge and/or skills

- Preparation of test report
- Evaluation of test results
- Evaluation of report as part of a larger audit on a system

### 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 consist of **one** type of evidence: product evidence.

The **product evidence** will relate to all outcomes (Outcomes 1 to 4). It must demonstrate the design (Outcome 2), implementation (Outcome 3) and evaluation (Outcome 4) of **at least one** real or hypothetical penetration test. Outcome 1 may be evidenced explicitly or implicitly; for example, the learner's knowledge of network security policies may be explicit or implicit in the artefact. The demonstration of knowledge and skills, evidenced by the product, should relate to the context of the specific penetration test. For example, identifying vulnerabilities (Outcome 2) will relate to a specific security scenario. If any knowledge or skill cannot be demonstrated in a specific scenario, there must be evidence that it was considered.

The security scenario may be **real or hypothetical**; if it is hypothetical, it must be **realistic**. The scenario may be **non-complex** but must provide scope for all (or most) of the knowledge and skills to be demonstrated.

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.

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

The SCQF level of this unit (level 7) provides additional context on the nature of the required evidence and the associated standards. Appropriate level descriptors should be used when making judgements about the evidence.

When evidence is produced in 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: Penetration Testing (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

The purpose of this unit is to provide information to the learner on the importance and relevance of penetration testing within the IT industry. Penetration testing is an integral part of cyber security with its importance rising considerably in recent years.

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**

This outcome is intended to provide an overview to the learner of penetration testing and cover the concepts of cyber security and cyber resilience. It is recommended that teachers take a broad approach in introducing the subject since it covers a number of different disciplines within IT. Dependent on the framework used to deliver this unit, then emphasis could be placed within that particular strand of the industry. For example, as part of the HND Networking, emphasis could be placed on identifying vulnerabilities in network devices (routers, switches). In software development, the emphasis could be placed on password protection and hashing or on the threat of SQL injections. The topics in the outcome are sufficiently broad to give the teacher the flexibility to investigate different strands within penetration testing.

Importance should be placed on how penetration testing has developed in recent years and the reasons behind the increase in demand. Discussions should also be encouraged regarding types of systems that should be tested, and when that testing should take place. It should also cover the testers themselves, with an emphasis on the different types of tests they perform. There are a number of penetration tests tools that can be used to demonstrate this kind of testing. Details of these sites are below. Time should also be spent on the importance of documenting penetration tests and evaluating results as part of a total test audit. Discussion should also be encouraged regarding the role of penetration testing in ethical hacking and legal implications.

## Higher National Unit Support Notes (cont)

## Unit title: Penetration Testing (SCQF level 7)

**Outcome 2**

Learners plan and prepare their own penetration test. This involves analysis of preliminary information (reconnaissance) and scanning target assets to identify vulnerabilities (discovery) within a particular network system/software. Learners are asked to analyse information and risks associated with this particular type of penetration test and to use appropriate tools (manual/automatic). They are then asked to design an appropriate test strategy, tests and test data to be used.

**Outcome 3**

This outcome gives learners the opportunity to run and document a penetration test. This is the most important step in penetration testing. Referred to as active intrusion attempts, penetration tests are used to verify potential vulnerabilities within a particular system. Dependent on the test itself, this could involve specialised operating system distributions for penetration testing, using automated security assessment tools, running SQL injections, cross-site scripting or any other recognised penetration test. Once run, these tests are documented and, if necessary, changes are made in order to secure the system and the tests run and documented again.

**Outcome 4**

This outcome gives learners the opportunity to prepare a test report. This report will cover both the testing procedures and analysis of vulnerabilities and risks. The report should include a summary of penetration tests, details of the steps and information gathered during the process. Details of the vulnerabilities and risks involved. Details of any changes made, cleaning and fixing of the system and suggestions for future security issues.

This unit itself will not cover complete National Occupational Standards (NOS). However, the content could contribute towards the larger NOS requirements, if taught with reference to the following organisational security requirements:

- TECIS60431: Contribute to information security testing activities.
- TECIS60441: Carry out information security testing activities.
- TECIS60451: Manage information security testing activities.
- TECIS60461: Direct information security testing activities.

## Guidance on approaches to delivery of this unit

This unit covers the underlying principles and methodology of designing and implementing a penetration test. It can be delivered in a number of different awards and should be flexible enough to let the centre place emphasis on their own particular areas. It is recommended that the knowledge outcome (ie, Outcome 1) is delivered first, followed by the knowledge statements of other outcomes.

Outcome 1 is a broad overview of the concepts behind penetration testing and would typically be delivered with lectures, online investigations and learner research. Outcomes 2, 3 and 4 cover the practical process of designing and implementing penetration tests. Since there are a wide range of these tests, then it may be beneficial for different groups to design and perform different tests and report their findings to the class. There are opportunities in Outcome 4 to evaluate the penetration test report as part of the wider remit of a security audit.

## Higher National Unit Support Notes (cont)

## Unit title: Penetration Testing (SCQF level 7)

There may be opportunities to integrate delivery, as well as formative and summative assessments, with other units. Within the HN Cyber Security, this unit would integrate well with both J0HK 34 *Ethical Hacking* and J0HD 34 *Scripting for Security*.

Penetration testing is evolving constantly to keep pace with cyber-attacks. Learners should be encouraged to research online up-to-date examples of penetration testing. They would also benefit from hearing, first hand, case studies from penetration testers themselves or through online presentations.

There are a number of online resources for Penetration Testing — listed below are a number of resources relevant at time of writing:

**https://www.tutorialspoint.com/penetration_testing/index.htm**
**http://www.pen-tests.com/penetration-testing-framework.html**
**http://www.softwaretestinghelp.com/penetration-testing-tools/**
**https://www.computerworld.com/article/2536045/endpoint-security/five-free-pen-testing-tools.html**
**https://www.tutorialspoint.com/penetration_testing/penetration_testing_vs_ethical_hacking.htm**

A suggested distribution of time, across the outcomes:

- Outcome 1 — 12 hours
- Outcome 2 — 12 hours
- Outcome 3 — 8 hours
- Outcome 4 — 8 hours

## 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.

The open-book assessment for this unit should be holistic. It could be undertaken using an e-portfolio, but it is recommended to be submitted as a report similar to what is handed over in industry to the client on completion of any kind of penetration test.

It is recommended that the learner is given a set scenario in order to design, implement and evaluate penetration tests. The scenario itself should be designed to suit the centre facilities. Centres are reminded that prior verification of centre-devised assessments would help to ensure that the national standard is being met.

Learners could create their own scenario and develop specific penetration tests for that scenario. Careful consideration must be given to the level of these scenarios and time constraints on completing the unit successfully.

Evidence for Outcome 1 should be contained in the introductory section of the report and cover the underlying principles of penetration testing, background research on tools and techniques and issues both ethical and legal in performing any form of penetration test.

## Higher National Unit Support Notes (cont)

## Unit title: Penetration Testing (SCQF level 7)

Evidence for Outcomes 2, 3 and 4 should be contained within subsequent sections detailing the design, implementation and evaluation of the penetration test. Along with the written report, appropriate screenshots, test logs, references, etc, should also be included.

To ensure authenticity, assessments should be submitted to Turnitin (a commonly used plagiarism tool used alongside Moodle VLE's to check learners' work against locally submitted work as well as internet materials).

Examples of penetration tests:

Web application tests: These tests look for security vulnerabilities in web-based applications and programs

Client-side tests: Intended to find vulnerabilities in and **exploit** client-side software (web browsers, media players, etc)

Network penetration tests: Involves finding target systems on the network, identify security issues with the design, implementation, and maintenance of servers, workstations, and network services

Wireless security tests: These tests involve discovering a target's physical environment to find unauthorized wireless access points or authorized wireless access points with security weaknesses

## 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

There is no automatic certification of core skills or core skills components in this unit. This unit does closely follow industry methodologies and practices regarding penetration tests, as well as putting into context the legal and ethical issues surrounding such tests, giving the learner the opportunity to develop their broader skills in both employability and citizenship.

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 5.

## History of changes to unit

| Version | Description of change | Date |
|---|---|---|
| 02 | Core Skills Component Problem Solving at SCQF level 5 embedded. | 31/08/18 |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

## General information for learners

## **Unit title**: Penetration Testing (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 is designed to introduce you to the principles and practice of penetration testing. It covers the underlying principles of penetration testing and details how a penetration test interacts with ethical hacking and legal issues. You will also find out about the online tools you can use to perform these tests. You will be given the opportunity to analyse and design test plans, set up test data, implement tests and evaluate the results.

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

- Describe the concepts underpinning penetration testing.
- Design a penetration test from a given scenario.
- Implement a penetration test from a given scenario.
- Evaluate a penetration test as part of a test audit.

The assessment for this unit will, most likely, be integrated for all four outcomes. You may be asked to produce a report on a penetration test, similar in structure to reports delivered to clients in industry.

This unit closely follows industry methodologies and practices regarding penetration tests and it puts into context the legal and ethical issues surrounding such tests. Therefore, you will also have the opportunity to develop broader skills in both employability and citizenship.

Progression from this unit could be further study on the subject itself, on the wider area of cyber security or on different forms of testing. You could also progress to other related HN qualifications.

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 5.