SQA Advanced Unit specification: general information

Unit title: Intrusion Prevention Systems

Unit code: HR8D 47

Superclass:	CC
Publication date:	August 2017
Source:	Scottish Qualifications Authority
Version:	01

Unit purpose

The purpose of this Unit is to introduce candidates to the threats faced by contemporary networks and the methods (and products) employed to mitigate these threats. The candidate will discuss the classes, features, methods and products employed under the heading Intrusion Prevention Systems.

1 Describe the features of Intrusion Prevention Systems.
2 Install, configure and test an Intrusion Prevention System.

Recommended prior knowledge and skills

Access to this Unit will be at the discretion of the Centre. The candidates would benefit from knowledge of fundamentals of computer servers, as well as the basic concepts of computer networking, security, the internet and associated services. Candidates should ideally possess at least the following SQA Advanced Units:

HR8G 47 *Network Concepts*
HP26 47 *Security Concepts*

Credit points and level

1 SQA 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 National 1 to Doctorates.*

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.

Unit specification: statement of standards

Unit title: Intrusion Prevention Systems

Unit code: HR8D 47

The sections of the Unit stating the Outcomes, Knowledge and/or Skills, and Evidence Requirements are mandatory.

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

Describe the features of Intrusion Prevention Systems.

Knowledge and/or Skills

- Describe Intrusion Prevention Systems.
- Describe types of Intrusion Prevention.
- Differentiate between various detection methods.

Evidence Requirements

Candidates will need to provide evidence to demonstrate their Knowledge and/or Skills by showing that they can:

- Define Intrusion Prevention Systems.
- Differentiate between types of Intrusion Prevention:
  - Network Intrusion Prevention Systems (NIPS)
  - Wireless Intrusion Prevention Systems (WIPS)
  - Host Intrusion Prevention Systems (HIPS)
- Defining one of the following detection methods:
  - Signature based
  - Anomaly Detection
  - Stateful Protocol Analysis

Outcome 1 can be assessed by using a case study where the candidate is given the role of presenting his/her research of the three selected IPS types to a group of company executives, where the importance and role of an IPS system within server technologies is stated.

The candidate must detail/define the need and concepts behind IPS systems. The candidate will also consider the three types of Intrusion Prevention, and then select two of the detection methods and use these findings as the basis of a report.

Outcome 2

Install, configure and test an Intrusion Prevention System.

Knowledge and/or Skills

- Install an Intrusion Prevention System.
- Configure the IPS for common attacks.
- Test the Intrusion Prevention System.

Evidence Requirements

Candidates will need to provide evidence to demonstrate their Knowledge and/or Skills by showing that they can:

- Install an Intrusion Prevention System.
- Configure the IPS for common attacks
- Test the Intrusion Prevention System for common attacks

Outcome 2 is by its nature a practical activity. The candidate will be expected to install, configure and test IDS they have installed. Configuration will be based on the usual attack areas, ie signature based, anomaly based or stateful protocol analysis.

The main emphasis for testing should be to remedy issues identified with the initial configuration carried out by the candidate. Identified issues could be missing out root, or e-mail header such as ‘free pictures’ or an attachment called ‘freepictures.exe’.

As this Outcome is practical a completed observation checklist, based on the specification provided or produced. Thus printouts of the initial configuration, testing logs and any changes to the original configuration will provide sufficient evidence to meet the Outcome.

Unit specification: support notes

Unit title: Intrusion Prevention Systems

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

The content of this Unit is aimed at providing the candidate with a broad knowledge base in the essentials of Intrusion Detection/Prevention Systems along with conceptual understanding of the elements in an intrusion detection/prevention system. There is also a practical emphasis with the candidate gaining hands on experience of the installation, configuration and testing of an Intrusion Prevention System (IPS).

There are two Outcomes in this Unit each of which is designed to introduce the candidate to different aspects of intrusion prevention systems.

The first Outcome introduces the candidate to the theoretical elements of IPS, where they will need to understand technologies such as traffic analysis, application protocol validation, and signature matching, along with focusing on what attack does, its behaviour, detect intrusions on the analysis of the traffic.

The second Outcome introduces the candidate to the practical elements of IPS systems their installation, configuration and testing. The candidate will install, configure and test the IPS. Any changes to the configuration as a result of testing should be documented and noted for evidence purposes.

Although the Unit is expressed in generic terms, it should be related to a real world context that will be familiar to candidates. The resources available within the delivering institution we dictate the type of IPS and testing software available for installation. However the student needs to be aware of a number of different IPS and testing software for other platform types.

Guidance on the delivery of this Unit

During the delivery of this Unit it is important that every opportunity is taken to introduce real-world examples, so there are opportunities for whole-class and group discussion and practical demonstrations wherever possible.

As this Unit has a theoretical component in Outcome 1 it will require the candidate to complete a significant amount of analysis and research before selecting the appropriate solution based on identified needs.

Concepts and terminology should be presented in context throughout the Unit. Video presentations should be used where appropriate for providing an alternative explanation of a difficult topic, or as a focus for class discussion or group work. Wherever possible theoretical learning should be re-enforced using practical demonstrations, for example to demonstrate the use of particular applications and tools.

Given the theoretical nature of Outcome 1 of this Unit, it is intended that a proportionate amount of time will be made available as a central part of the course for revision, tutorials and formative assessment exercises. Candidates should be strongly encouraged to undertake further reading, opportunities for individual or group research should be provided.

Outcome 2 is practical and will require the candidate to install, configure and test the selected IDS system. For practical purposes candidates should be exposed to up-to-date IDS systems and testing tools. While the exact time allocated to this Unit is at the discretion of the centre, the notional design length is 40 hours. A suggested allocation of time is:

Analysis and research	10 hours
Report or Presentation	5 hours
Installation and configuration of IDS	15 hours
Testing	5 hours
Finalising/ remediation	5 hours

Guidance on the assessment of this Unit

Outcome 1

Describe the features of Intrusion Prevention Systems

The candidate needs to be able to define the concepts and issues raised by the selection of an appropriate Intrusion Detection/Prevention Systems. Emphasis should be placed on the types of protection/detection systems that can be utilised within an organisation. So the candidate needs to be aware of:

- Network Intrusion (NIPS)
- Wireless Intrusion (WIPS)
- Host Intrusion (HIPS)
- Protocol Analysis
- Rate based (RBIPS)

The types of detection methods should be explored and the candidate **will define two of the detection methods.**

Outcome 1 can be assessed by using a case study where the candidate is give the role of presenting his/her finding to a group of company executives where they explore and explain the importance and role of an IDS system. This could be carried out by completion of a report of approximately 800 words.

Outcome 2

Install, configure and test an Intrusion Prevention System

Candidates will need to provide evidence to demonstrate their Knowledge and/or Skills by showing that they can:

- Install an Intrusion Prevention System (IPS).
- Configure the IPS for common attack vectors
- Test the Intrusion Prevention System and reconfigure identified issues.

Outcome 2 is by its nature a practical activity. The candidate will be expected to install, configure and test IPS they have installed. In terms of the specification, this can be produced or specified as part of Outcome 1 or can be provided by the tutor.

The type of IPS employed, will of course be based on the underlying hardware facilities available at the delivering institution. There is a wide choice of Windows and Unix/Linux based systems available which will meet the required features for configuration. The candidate needs to understand the common methods of attack that may be utilised.

In terms of testing the candidate should use a testing tool to check the effectiveness of their configuration against penetration, integrity and availability attacks. Again there are various tools available both for windows and Unix/Linux based systems to allow the testing to be carried out. So tools like FTester, Tomahawk or IDs Wake up could be utilised by the candidate. This is not an exhaustive list so other testing tools are also acceptable.

As this Outcome is practical a completed observation checklist, based on the specification provided or produced is required. Thus printouts of the initial configuration, testing logs and any changes to the original configuration will provide sufficient evidence to meet the Outcome.

Online and Distance Learning

It is perfectly feasible to develop a range of blended learning material to deliver this Unit by online and distance learning means. Support for distance learners could be provided by both synchronous and asynchronous communication technologies.

For the practical elements this may be carried out by utilising a virtual server, which the candidate may use for the installation, configuration and testing aspects of Outcome 2.

Care would need to be taken to ensure the authenticity of the assessments undertaken by online or distance learners for Outcome 1 and 2.

Opportunities for developing Core Skills

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

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.

History of changes to Unit

Version	Description of change	Date

SQA acknowledges the valuable contribution that Scotland's colleges have made to the development of SQA Advanced Qualifications.

FURTHER INFORMATION: Call SQA's Customer Contact Centre on 44 (0) 141 500 5030 or 0345 279 1000. Alternatively, complete our Centre Feedback Form.

General information for candidates

Unit title: Intrusion Prevention Systems

The content of this Unit is aimed at providing you with a broad knowledge to the threats faced by contemporary networks and the methods (and products) employed to mitigate these threats. So you will discuss the issues, features, attack methods and products employed under the generic heading Intrusion Detection/Prevention Systems.

During the Unit you will

- Describe the features of Intrusion Detection/Protection Systems
- Install, configure and test an Intrusion Detection/Protection System

The content of this Unit is aimed at providing you with a broad knowledge base in the essentials of IDS installation, configuration and testing along with conceptual understanding of the elements associated with Intrusion Prevention or Detection.

During the Unit you will learn about the various type of intrusion prevention systems that are available for the different types of computing platform, how they are utilised and their benefits. Practical elements will involve you in installing, configuring and testing an IDP system.

On completion of the Unit you will be able to:

1 Describe the features of Intrusion Prevention Systems.
2 Install, configure and test an Intrusion Prevention System.

Outcome 1 of the Unit covers the theoretical information required for you to consider the specification of an IPS for a fictitious company.

You will, for example, evaluate the different IPS elements, detection methods and common attacks carried out on web based servers.

Outcome 2 will introduce you to the skills required for installing, configuring, and testing the IPS software. You will also learn how to configure the IPS based on the needs of perceived security issues. You will also be required to test the IPS system that you have installed.

To meet the assessment requirements of this Unit you will write a short report for Outcome 1 consisting of 800 words. Outcome 2 will be assessed by production of configuration printouts and test logs along with a completed observation checklist.