Higher National Unit Specification

General information

Unit title: Scripting for Security (SCQF level 7)

Unit code: J0HD 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 practice of security scripting and how it is used by security specialists and malicious individuals. This is a **specialist** unit, intended for learners who have an interest in computing. It is particularly suitable for learners who have an interest in cyber security, computer networking/hardware, and software development.

This unit covers the basis of scripting in cyber security and will focus on the uses of scripting languages, and the types of devices that can be used regarding security scripting. The unit will explore the implications of scripting and how we can reduce the risk of scripts being run on everyday devices used by organisations.

The unit will also focus on how scripts can be used to the good, and how software can help non-professionals and professionals be more efficient in their roles.

On completion of this unit, learners will understand the implications of scripts and the effects that these scripts can have on individuals and organisations. The learner will also know how to create a security program to allow non-security professionals to undergo a security role with ease.

Learners may progress to J0HB 34 *Penetration Testing*, J0HK 34 *Ethical Hacking*, or J0HF 34 *Social Engineering* at SCQF level 7.

Higher National Unit Specification: General information (cont)

Unit title: Scripting for Security (SCQF level 7)

Outcomes

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

1 Identify the usage of different devices used in security scripting.
2 Use an appropriate scripting language in relation to cyber security.
3 Construct a security program for non-security professionals to meet the requirements of a brief.

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. However, it would be beneficial if learners possessed some knowledge of software development or ethical hacking.

This may be evidenced by possession of a relevant software coding unit, particularly in Java, Python or similar, such as HY2C 46 *Computer Programming*, or a unit with some knowledge of coding (particularly in Kali Linux), such as H9HY 46 *Ethical Hacking*.

Core Skills

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

Complete Core Skill None

Core Skill component Critical Thinking 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.

If learners do not possess any knowledge of ethical hacking or software development, then it is recommended that this unit be delivered alongside a relevant *Software Development* unit and an *Ethical Hacking* unit.

A suitable software development unit would be H17X 34 *Software Development*: *Programming Foundations* or J0HA 34 *Computer Programming*.

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: Scripting for Security (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

Identify the usage of different devices used in security scripting.

Knowledge and/or skills

- Definition of security scripting
- Types of devices used in security scripting
- Types of scripting languages used in cyber security
- Ways of using security devices/scripts in a malicious/ethical manner

Outcome 2

Use an appropriate scripting language in relation to cyber security.

Knowledge and/or skills

- Software variables, including Var and Const
- Software statements, including IF statement
- Software constructs, including While Loops, For Loops
- Software Operations, including Boolean Logic

Outcome 3

Construct a security program for non-security professionals to meet the requirements of a brief.

Knowledge and/or skills

- Understanding of a client brief
- Good programming practice (comments)
- User menu
- Functions and objects

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 two forms.

1 Knowledge evidence (Outcome 1)
2 Product evidence (Outcomes 2 and 3)

Higher National Unit Specification: Statement of standards (cont)

Unit title: Scripting for Security (SCQF level 7)

The **knowledge evidence** will relate to Outcome 1. It will comprise the knowledge required in Outcome 1. Knowledge evidence is required for all knowledge and/or skills statements except those explicitly relating to skills. The following knowledge must be demonstrated:

- Explain what is meant by security scripting
- Research security devices are used in security scripting (**at least** four)
- Explain why security devices are used in security scripting
- Identify ways in which security devices/scripts are used in a malicious/ethical manner (**at least** three)
- Identify the different scripting languages used in cyber security (**at least** four)

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 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 **product evidence** will relate to Outcomes 2 and 3. It will demonstrate the learner's ability to create a security script that can help a non-security professional undertake a cyber security task.

The security script produced by the learner must exhibit the following:

- Use of variables
- Use of constructors
- Use of IF statements
- Use of Loops (For Loops, While Loops, etc)
- Use of Boolean Logic (True, False)
- Be user friendly
- Meet all of the client's specifications
- Use commenting where required
- Have a user menu that the client can use to help undertake cyber security tasks
- Use functions appropriately that are called by the user menu
- Have common security tasks implemented into the program (port scanning, packet sniffing, etc)

Learners must demonstrate that they can read and understand a client brief. The learner should create a security program for a client that will help them undertake common security tasks.

This evidence be produced in lightly controlled conditions over an extended period of time, with access to resources and reference materials. The evidence must be produced by the learner, without assistance.

The product evidence criteria will differ depending on the type of scripting language used by the centre; alternatively, this can be done in a virtual environment. More information will be provided in the support notes.

Higher National Unit Specification: Statement of standards (cont)

Unit title: Scripting for Security (SCQF level 7)

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 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: Scripting for Security (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 for learners to create a security script that can be used by an individual to perform cyber security in a professional and ethical manner. The unit also aims to help learners understand why these scripts can be the perfect weapon for malicious individuals.

The term *script kiddies* was created to define the malicious individuals who would use security scripts to attack a machine/device, or use a script to find and exploit the vulnerability on a machine/device.

This unit is intended for learners who have an interest in software development, programming or cyber security. The unit is designed for learners who want to go into an area of expertise where cyber security is important, and it is designed in a way that learners can go for a role in software development where they may be responsible for creating a program/script that will then be given to an organisation. However, the unit may be suitable in a variety of courses that offer any of these disciplines.

It is recommended that this unit be delivered alongside other units covering software development/scripting and/or computer hardware, but this is entirely up to the discretion of the centre delivering the unit.

If the unit was delivered alongside a software development unit, this would allow learners to understand the security implications that these scripts can have and consider this when they are creating their software/websites.

Moreover, if the unit was delivered alongside a hardware unit focusing on cyber security, this could show learners some of the implications that scripts have on their network and how security scripts could allow them to be more efficient in their jobs.

Centres are free to use a coding language of their choice, such as Python, C++, PHP, HTML, Ruby, Visual Basic (VB), Java, JavaScript, Perl, Bash or even PowerShell, as long as the criteria set out in the evidence requirements section are met.

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.

Higher National Unit Support Notes (cont)

Unit title: Scripting for Security (SCQF level 7)

Outcome 1

Outcome 1 focuses on security scripting and what is meant by security scripting. By understanding this concept, learners will have a better understanding of the implications of security scripting. They will gain a better understanding of the devices used in security scripting, such as rubber duckies, Raspberry Pis, PowerShell, Servers, USBs, or any device that can run a scripting language, which can be used to attack a device.

The learners will focus on languages that can be used in security scripting, such as Bash, Shell, Java, JavaScript, Python, PHP, HTML, C++, SQL, Perl, Ruby and Visual Basic (VB). Centres are free to use other languages if they can meet the criteria set in the Evidence Requirements section.

The final part of Outcome 1 will allow learners to focus on how these scripts are used by malicious individuals and professionals. The learner will look at examples of scripts that have been used in the past for malicious uses, NSA Tools, Petya and WannaCry, and they will also focus on scripts that can be used to the good, such as tshark, Python Sockets and more.

The learner will also explore the implications of these attacks to develop a better understanding and help them become better cyber security professionals.

Outcome 2

Outcome 2 focuses on the software development side of the unit and introduces the learner to the concepts of software developing/scripting. The learner will look at the different variables used in coding languages, such as const, var, global, etc.

As well as statements, the learner will focus on how these are used, and will use common statements such as IF, Else, Elseif, to make the program more adaptable and user friendly, and to catch any errors or inputs from the user.

Learners will also use different types of loops, for example, a While Loop that will keep looping until a certain condition has been met; a For loop which will only run for a specified amount of time; and other loops that can be used in the creation of the script.

The final thing learners will focus on is Boolean Logic. This is True or False statements, and using some of the methods mentioned above with Boolean logic, learners can make a fluent script that will allow them to chain other constructs onto each other.

Outcome 3

Outcome 3 will focus on the learner's ability to read a client brief, which will specify what their security program/script must do for the user. The finished product must be user friendly so it can be used both by professional and non-professional individuals.

The script must have appropriate commenting to allow other people to understand what is happening in the script, and the user must have an option to pick what test they want to run. This must take the form of a user menu, which could be a simple menu using a number system, or a more advanced menu using graphics and buttons. This is entirely at the discretion of the learner/centre.

The code produced by the learner must have constructs that are called by the user menu, and these should be common tasks that the user may want to run, such as port scanning, ping tools, traceroute, vulnerability scanning, checking if a website is available, etc.

The learner must ensure that these tasks are common tasks that the user may want to use and it is at the discretion of the educator/centre to define what is classed as common tasks, but they must be related to cyber security, network monitoring or troubleshooting.

Guidance on approaches to delivery of this unit

This unit can be delivered in a number of different group awards that could meet the criteria of the evidence requirements section. This could be web development, software development, hardware, networking or even cyber security.

Outcome 1 will focus on research and will require the learner to research the different scripting languages, devices and effects of these. Educators could deliver this outcome using PowerPoints and a series of tasks that allow the learner to do some research. The learner can use examples of security attacks that have used security tools/scripts.

These attacks would need to have been carried out by malicious individuals and have caused damage to an organisation and their reputation. The educator could use case studies and examples to help with the teaching.

Outcomes 2 and 3 should be delivered together. Centres are free to use the coding language of their choice, and the educator could allow the learner to create some small programs that will introduce them to the basics of the coding language that they are using. These programs could be simple scripts such as hello world, magic eight ball, and other programs that are appropriate and help deliver the learning.

Centres could then progress onto more advanced programs, to which the educator could add some menus to make the programs more interactive and user friendly, with the basis on commenting to make the code easy to follow and understand.

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

Outcome 1: 12 hours
Outcome 2: 14 hours
Outcome 3: 14 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.

Higher National Unit Support Notes (cont)

Unit title: Scripting for Security (SCQF level 7)

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.

Suggestions for the knowledge requirements for Outcome 1 could take the form of a written or oral test that would demonstrate that the learner has achieved all the knowledge and skills statements for Outcome 1.

The assessment should last no more than 60 minutes and be closed-book, without access resources or reference materials. The assessment could take the form of oral questioning with a set amount of questions.

If written evidence is used, the centre can use selected response questioning with a pass mark of 60%, or extended response questioning. The assessment should be attempted on a single occasion.

If re-assessment is required, the centre must use a different sample of questions or responses.

Each sample must include the following:

- At least four devices that can be used for security scripting
- At least four scripting languages that can be used for security scripting
- Definition of security scripting
- At least three ways in which security scripts can be used in a malicious/ethical way

The evidence requirements for Outcomes 2 and 3 could be sampled in a variety of ways. This could take the form of a blog/journal, where sampling would be taken from the activities undertaken in the classroom.

The learners could create a security script that demonstrates the evidence requirements have been met. Alternatively, learners could create a series of scripts that would demonstrate that all of the knowledge and skills statements for Outcomes 2 and 3 had been achieved.

Centres are free to use whatever method of assessment they want, as long as the following evidence criteria has been met:

Outcome 2

- Use of variables
- Use of constructors
- Learners understand and use IF statements
- Evidence that the following Loops have been used (For Loops, While Loops, etc)
- Examples of Boolean Logic (True, False)

Outcome 3

- Meets the requirements of the brief
- Is user friendly, the script must be easy to use and can be used by anybody
- Uses commenting where required
- Evidence of a user menu being used
- User menu must be associated with functions that are called by the user menu
- Has common security tasks implemented into the program (port scanning, packet sniffing, etc)

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.

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

There are opportunities to develop the following Core Skills throughout this unit:

- *Communication*
- *Information and Communication Technology*
- *Problem Solving*
- *Working with Others*

Higher National Unit Support Notes (cont)

Unit title: Scripting for Security (SCQF level 7)

Throughout all of the outcomes, learners will gain an understanding of how to communicate effectively. Centres may wish to use presentations to teach the learners about security scripting; this would give learners an opportunity to respond to questions asked.

While undergoing the security scripting element, the learners will have the opportunity to ask a client about the specification and can gain more information on what is required from the educator.

Learners will also be working with computer systems and this will enhance their skills in ICT; they may be asked to write a report as part of their performance criteria of the security script.

They will gain an understanding of problem solving through the coding element of the unit. They will be required to create a security script that can perform certain tasks, which will involve problem solving through rectifying errors and issues in their script.

Throughout Outcomes 2 and 3, centres may wish to encourage group work, which would allow learners to enhance their team working skills. They will be collaborating with the clients to ensure that the criteria is met; centres may be able to work with external companies that may require a security script made for them which will give them a real-life scenario and develop their team working skills further.

This Unit has the Critical Thinking component of Problem Solving embedded in it. This means that when learners achieve the Unit, their Core Skills profile will also be updated to show they have achieved Critical Thinking at SCQF level 5.

History of changes to unit

Version	Description of change	Date
02	Core Skills Component Critical Thinking at SCQF level 5 embedded.	31/08/18

General information for learners

Unit title: Scripting for Security (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 introduce you to the concepts of security scripting and how it can be used maliciously and ethically. It is suitable for learners who have an interest in cyber security, networking or software development.

The unit covers the concepts of security scripting, the different types of scripts that can be used in security scripting. Although it is not essential, it would be advantageous if you had some previous knowledge of software development or are undertaking a software development unit alongside this one. It would also be beneficial if you had some knowledge of networks and how they work, especially knowledge of IP addressing and sub-netting.

This unit covers the following:

- The definition of security scripting
- The different types of devices used in security scripting
- The different types of scripting languages used in cyber security
- How security devices/scripts are used in a malicious/ethical way

It also teaches you how to use the following, in relation to security scripting:

- Software variables (var, constants)
- Software statements (IF statement)
- Software constructs (while loops, for loops)
- Software operations (Boolean Logic)
- How to understand a client brief
- Good programming practice (comments)
- How to implement a user menu
- Different functions and objects and their uses

Each topic will be explored in detail through the use of theory and practical tasks. These will allow you to understand the concepts in a real-life scenario and will simulate the types of things you may need to do in the industry. There will be an emphasis on research at the start of the unit, which will give you experience in researching if they have never done it before.

The theory for this unit will, most likely, be assessed with a multiple-choice test, and the practical may be assessed in a variety of ways, which could include practical tasks, videos, witness statements, reports, logbooks or any other way deemed by your educator.

On completion of this unit, you will understand how security scripting can make a job easier, you will understand the concepts of coding and security scripting, and by understanding the languages that can be used for security scripting, you will be able to put better controls in place to reduce the risk of malicious scripts from running on your networks.

This Unit has the Critical Thinking component of Problem Solving embedded in it. This means that when you achieve the Unit, your Core Skills profile will also be updated to show you have achieved Critical Thinking at SCQF level 5.