Unit 4 - Extended Project: Defending an Online System

Overview

The candidate can plan and execute the installation and setup of a secure website for a specified purpose, such as a Moodle VLE or Wordpress blog for a school department. They will research a number of working systems to see how they functions and choose one that is most suitable. They will plan how to install and configure a site based on a number of conditions, and execute that plan. They will test the system against some predetermined attacks and make sure it is as secure as can be. They will then evaluate the process and document it as well as make some recommendations for others.

A work activity will typically be 'non-routine or unfamiliar' because the task or context is likely to require some preparation, clarification or research to separate the components and to identify what factors need to be considered. For example, time available, audience needs, accessibility of source, types of content, message and meaning, before an approach can be planned; and the techniques required will involve a number of steps and at times be non-routine or unfamiliar.

Example of context – setting up a system and making a detailed report and presentation to show how safe and secure it is.

Assessor's guide to interpreting the criteria

General Information

RQF general description for Level 2 qualifications

- Achievement at RQF level 2 (EQF Level 3) reflects the ability to select and use relevant knowledge, ideas, skills and procedures to complete well-defined tasks and address straightforward problems. It includes taking responsibility for completing tasks and procedures and exercising autonomy and judgement subject to overall direction or guidance.
- Use understanding of facts, procedures and ideas to complete well-defined tasks and address straightforward problems. Interpret relevant information and ideas. Be aware of the types of information that are relevant to the area of study or work.
- Complete well-defined, generally routine tasks and address straightforward problems. Select and use relevant skills and procedures. Identify, gather and use relevant information to inform actions. Identify how effective actions have been.
- Take responsibility for completing tasks and procedures subject to direction or guidance as needed.

Requirements

- Standards must be confirmed by a trained Gold Level Assessor or higher.
- Assessors must at a minimum record assessment judgements as entries in the on-line mark book on the INGOTs.org certification site.
- The work in the unit is recommended in order for candidates to have covered enough depth and breadth in the topic to successfully carry out their controlled assessment and take the external exam.
- When the candidate has covered as much of ths material as necessary to complete the controlled assessment element, they may be introduced to the topic
- This unit should take an average level 2 learner 45 hours of work to complete.

Assessment Method

Understanding of these learning objectives will be demonstrated through answering questions related to key ideas and concepts in the terminal examination as well as practical application of their understanding through the controlled assessment.

Expansion of the assessment criteria

1.Research a working cyber security system

1.1 I can investigate a working system to determine the main components

Learners should be able to demonstrate they understand what the main parts of a web based system are

Additional information and guidance
For this project, students will be required to build a basis web based system. In most cases this will be based on a LAMP structure as this would be the easiest to recreate and also since 80% of the existing Internet runs on this type of platform it would be useful for their future studies and career choices. For this, they are required to read up and understand what it is they will be working with.

A LAMP based system consists of:

- A Linux operating system
- An Apache web server application
- A MySQL database
- A PHP application for communication between the database and the web front end

There are variations on this basic theme as they will discover in their research and they need to be clear they have made the right choices as far as possible. They could use a WAMP (Windows) based system if they are more familiar with this set-up, but this might involve licensing issues.

1.2 I can explain the main system components

Learners should be able to demonstrate they understand each of the main system components

Additional information and guidance
As identified in 1.1 above, the main components of a working web based system will be build around

a Linux operating system. These systems are easy to obtain and are free so offer the best flexibility and accessibility for this qualification. There are many flavours of Linux available but the most common are: Debian/Ubuntu; RedHat and SuSE. Each of these have spin offs such as CentOS, the community version of RedHat or OpenSuSE, the community version of SuSE. Their main differences are in the way that they handle “packages” or the files and libraries used to make the system run.

Students can give an overview of the main components and depending on how interested they are they can either provide a table of basic details or a more detailed report. For this criteria, they can also explain variations on the basic LAMP theme. The most popular web server is Apache, but there is also Nginx which is believed to be better for large scale deployments. The MySQL database has a number of variants, such as the Mongo or Maria versions and increasingly people are using a NoSQL systems as the amount of data being handled and the quickly changing nature of it makes “old” database structures not agile enough. PHP (Hypertext Preprocessor) is a software application that acts as a link between the web front end and the backend applications (web server and database). It incorporates tool which help to speed up the rendering of websites and the capture and storage of data, such as with online web forms.

1.3 I can describe how the components fit together

Learners should be able to demonstrate they understand the relationship between the main components

Additional information and guidance
The various components, over time, have evolved to work quite closely together. Each of the main applications has various library files that allow them to work together. For example, there is a set of php files that allow it to work with the web server and database, such as the file php-mysql which allows php to access a MySQL database structure, or libapache2-mod-php which is a module that connects Apache to PHP code. Students could create their own diagram to illustrate their understanding.

https://en.wikipedia.org/wiki/LAMP_%28software_bundle%29#/media/File:LAM... [1]

1.4 I can make detailed notes of my findings

Learners should be able to demonstrate they can research and keep useful notes on their findings

Additional information and guidance
Most people that work in the security based industries will keep some kind of notes in order to help them be more effective or efficient. It may be that a small paper based notebook is the safest and most accessible. If they use an online system, given the nature of what they are doing which involves security based information, they need to make sure it is robust and secure. A summary of their findings will be useful for further reference and study.

1.5 I can present my notes to an audience for feedback

Learners should be able to present their findings

Additional information and guidance
The presentation does not have to be a formal one to a large audience and could be in the form of a weekly meeting as part of a security team they are part of. This can be facilitated by the assessor and allow students to discuss their findings and agree on ideas and principles. If a system is set-up for tracking what they are doing, such as a support system, they can use this to discuss their findings.

1.6 I can list some of the key objectives of the system I will design

Learners should be able to create a working list of some objectives to act as a design guide

Additional information and guidance

(function(i,s,o,g,r,a,m){i['GoogleAnalyticsObject']=r;i[r]=i[r]||function(){ (i[r].q=i[r].q||[]).push(arguments)},i[r].l=1*new Date();a=s.createElement(o), m=s.getElementsByTagName(o)[0];a.async=1;a.src=g;m.parentNode.insertBefore(a,m) })(window,document,'script','//www.google-analytics.com/analytics.js','ga'); ga('create', 'UA-46896377-2', 'auto'); ga('send', 'pageview');

The list of objectives is likely to be dynamic as they begin working on their system and finding out what works and what doesn't. At this stage they need to be able to set some simple objectives to work towards. This could be as basic as what flavour of LAMP or WAMP they settle on and what they hope to achieve by this. They might have more detailed objectives such as achieving a certain level of user concurrency (the number of people accessing the same material at the same time). This will involve thinking carefully about the system resources. High levels of concurrency will require a server with a powerful processor, lots of RAM and a fast hard drive.

Some of the objectives will be:

- Decent access speed (maybe use some testing facility to gauge the speed of page loads)
- Secure against X% of common threats
- Secure against DDoS attacks
- Secure against root access
- Compatible with current technologies
- Compliant with current security standards
- Secure against commonplace external compromises, injection attacks or poorly crafted software exploits

2.Plan to build a cyber safe web site or server

2.1 I can make a working skeletal plan of a system

Learners should be able to create a plan of how the system will be made and secured

Additional information and guidance
The first phase of this process is to produce a plan of action and to highlight what is required in terms of equipment, resources, materials and knowledge to get the job done. A useful plan might include a diagram of how the system will fit together and some of the important points that need extra attention, such as roles and permissions and configuration settings. As soon as a site goes live on the internet it is being hit, so it is important to plan the timing of various activities to make sure it is not compromised before it can be properly defended. What is the order of activities and what activities depend on each other. For example, can you install the web server without having a database or PHP already installed? It might be useful for students to use a SMART plan for this process:

Specific - I will install MySQL version 5.X as it is required by version X of x software
Measurable - I will be able to stop 80% of threats such as root access attempts
Achievable - I will create one working web site to allow a membership of 30 people
Realistic/Relevant - I will make a site that will be as secure as possible with my existing knowledge
Time-bound - I will complete the project within 20 weeks of work

2.2 I can set clear objectives and outcomes to build a system

Learners should be able to demonstrate they understand what a system should be capable of in terms of outcomes and objectives

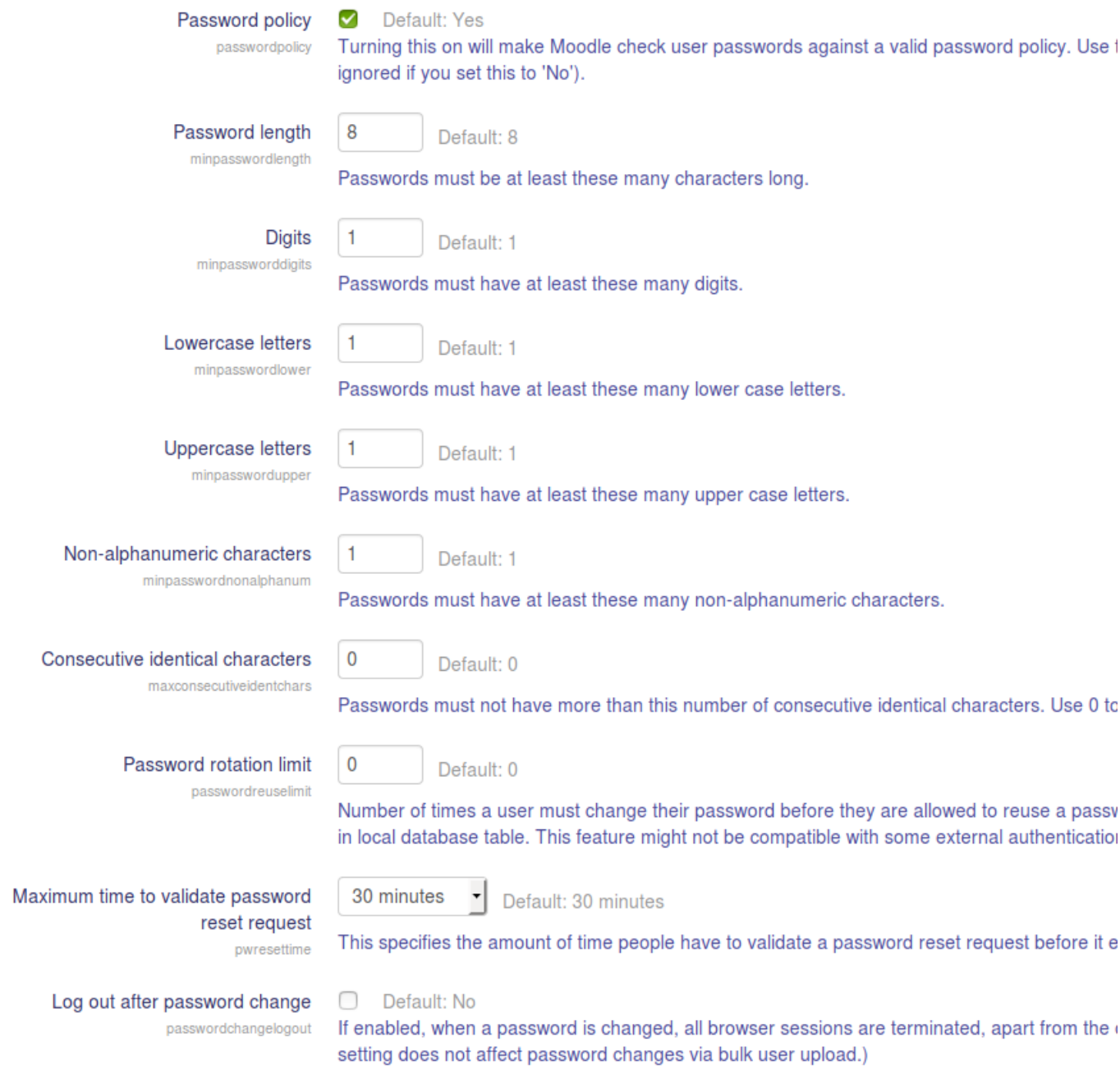
Additional information and guidance
Learners need to be realistic that there is no such thing as a perfect system, but if they do their research well and think through the various options, they should be able to solve many of the issues related to security. The objectives for the system will need to be understandable for someone who is not as well researched as they are and they be replicable by following whatever documentation they make. They could set out some objectives to prevent the site being compromised by some sort of injection or someone posting spam on the site. Other objectives might be to prevent someone gaining access to the site to use it a a php mail server or similar. The objectives will therefore determine the outcomes. The outcomes will be what they consider to be a success factor. Some of the outcomes might be to not see specific IP addresses in the log files, if they set up the system to block these. It might be that the logs show that people trying to get into specific areas are turned

away and disappear as they give up. The objectives and outcomes will vary depending on the nature of the system they are developing.

2.3 I can list the main safety features that will need to be addressed for success

Learners should be able to demonstrate they understand the basic security required for their site to be a success

Additional information and guidance
The primary focus here will be on the user experience, so they are not compromised by their details being taken or shared. This means that the roles and permissions of users of the site are well configured so that people can't pretend to be someone else or get elevated access rights to start abusing others. For the system itself, it means the database and web server can't be attacked and compromised and data stolen, or that the underlying server can't be hacked into and used for illicit purposes. One classic problem for many websites is that the customer does not want to have complex passwords to remember and they are given admin rights, so they automatically change it to something easy which makes it a prime target for hacking and password cracking. At the very least a site should have a decent password policy for users, especially if they have elevated rights and permissions.



2.4 I can explain the main hardware requirements needed

Learners should be able to explain the main aspects of the underlying hardware

Additional information and guidance
As with your home computer or mobile phone, the more power and resources you have, the more you are able to achieve in less time.

A server has to carry out tasks, such as serving web pages or doing detailed queries on a database to process for a web page. All of these take different amounts of time and power. A web site that is heavy in graphics with a great deal of interactive content will take a lot of processing power and while it is being processed, some amount of the data will be held in RAM. Some of the data will need to be pulled from hard drives. All of these will have their own characteristics which will affect performance and need to be considered. Learners need to have a good understanding of these main characteristics, at least to make basic recommendations. The key point here, especially with online systems, is that this will all cost money. If the system needs to be powerful with lots of RAM and hard drive space, and requires a level of management such as backups and patching, this will all cost.

A blogging system such as Wordpress has mostly software based requirements such as the latest PHP or MySQL etc. A more data intensive system such as a VLE like Moodle has requirements related to use, so as far as hardware:

- Disk space: 200MB for the Moodle code, plus as much as you need to store content. 5GB is probably a realistic minimum.
- Processor: 1GHz (min), 2GHz dual core or more recommended.
- Memory: 512MB (min), 1GB or more is recommended. 8GB plus is likely on a large production server
- Consider separate servers for the web "front ends" and the database. It is much easier to "tune"

2.5 I can explain the main software aspects of the system

Learners should be able to demonstrate they understand the different applications they need and what their choice will mean

Additional information and guidance
As mentioned in 2.4 above, most applications will give minimum requirements for hardware and software as required. The software will be the basic AMP set-up, but could have specific needs, such as the need for PHP 7 in the latest versions of software such as Wordpress. For this criterion, learners need to just show that they have a working knowledge of these main systems. They should appreciate the advantages of newer versions of software packages, but be able to weigh these against stability and security concerns.

Many software packages are dependent on other underlying aspects of hardware. For example, the Debian based Linux operating system is updated against key components like the kernel. The derivative Ubuntu system updates the system every 6 months, but has a LTS (Long Term Support) version which is supported with fixes and patches for at least 5 years. These LTS versions might not have the latest versions of Apache or PHP, but may be good enough for the learner’s needs.

2.6 I can make a final plan for the system

Learners should be able to demonstrate the ability to put together a workable and functional plan of action

Additional information and guidance
Before learners begin to build their system, they should have worked out how and when they will do this. Thy will need to have a set of guidelines for the materials they need, some of the configuration

settings and perhaps some of the likely problems they may encounter. The plan should have some indication of the order to development and a rough idea of some of time allowances. All of this detail can be used at a later point to refer back to for improvements, but also helps in case there are any problems. If problems do occur, with a detailed plan it is easier to trace backwards to try and work out at what point the error was introduced.

One the plan has been finalised and signed off, either by the assessor or a client, work can then begin.

3.Develop a cyber safe web site or server

3.1 I can prepare a system in terms of specifications

Learners should be able to demonstrate the ability to prepare a system for build in terms of hardware and software needs

Additional information and guidance
The final system build will depend on some key needs of the user as well as the learner's understanding of security. If the system is working as part of an Intranet, the needs will be different compared to a public facing server running software that anyone can access and create accounts on. If the system is for a client in the local community, they will not have the robust security layers of a large organisations and extra steps will need to be taken.

The preparation here is in getting a system ready for the installation and set-up of the main application, but also the generic security preparation.

- Does it have the right amount and type of RAM to run the processes effectively.
- Is there enough storage.
- Is the storage fast enough
- What partitions are required
- What kind of operating system is required, i.e. LTS or more recent versions
- What versions of the key components are required: PHP, MySQL etc.
- Is there peripheral equipment used such as routers and switches

These are some of the issues that require some preparation procedures.

3.2 I can explain the specification in terms of performance needs

Learners should be able to explain the choices made in terms of performance

Additional information and guidance
With any computer based system, there is always a number of trade offs. There may be a need for speed, but also for energy efficiency. What will the trade off be. The more power a system generates, the more need there is for good maintenance and proactive fixes. If there are some bottlenecks, how are these overcome. Small companies in rural areas may not be able to run their own web server’s because their download and upload speeds are too low to be effective.

Learners should be able to put together a short report highlighting the key elements of their proposed system as they build it in terms of performance. It does not have to be hugely detailed, but should show that they have considered some of the key issues above. For example, they may say that they have chosen an older version of a Linux operating system as the long term stability was important and the security levels more manageable, even though this means that an older and slower version of PHP has to be used. In most cases, the security will be central. The older version of PHP may be slower, but will be more mature and therefore less prone to security bugs. However, they also need to bear in mind end of life issues.

There needs to be an understanding that at some point in the future an operating system of key

piece of software will no longer be supported and security patched and a move to a newer system will be required.

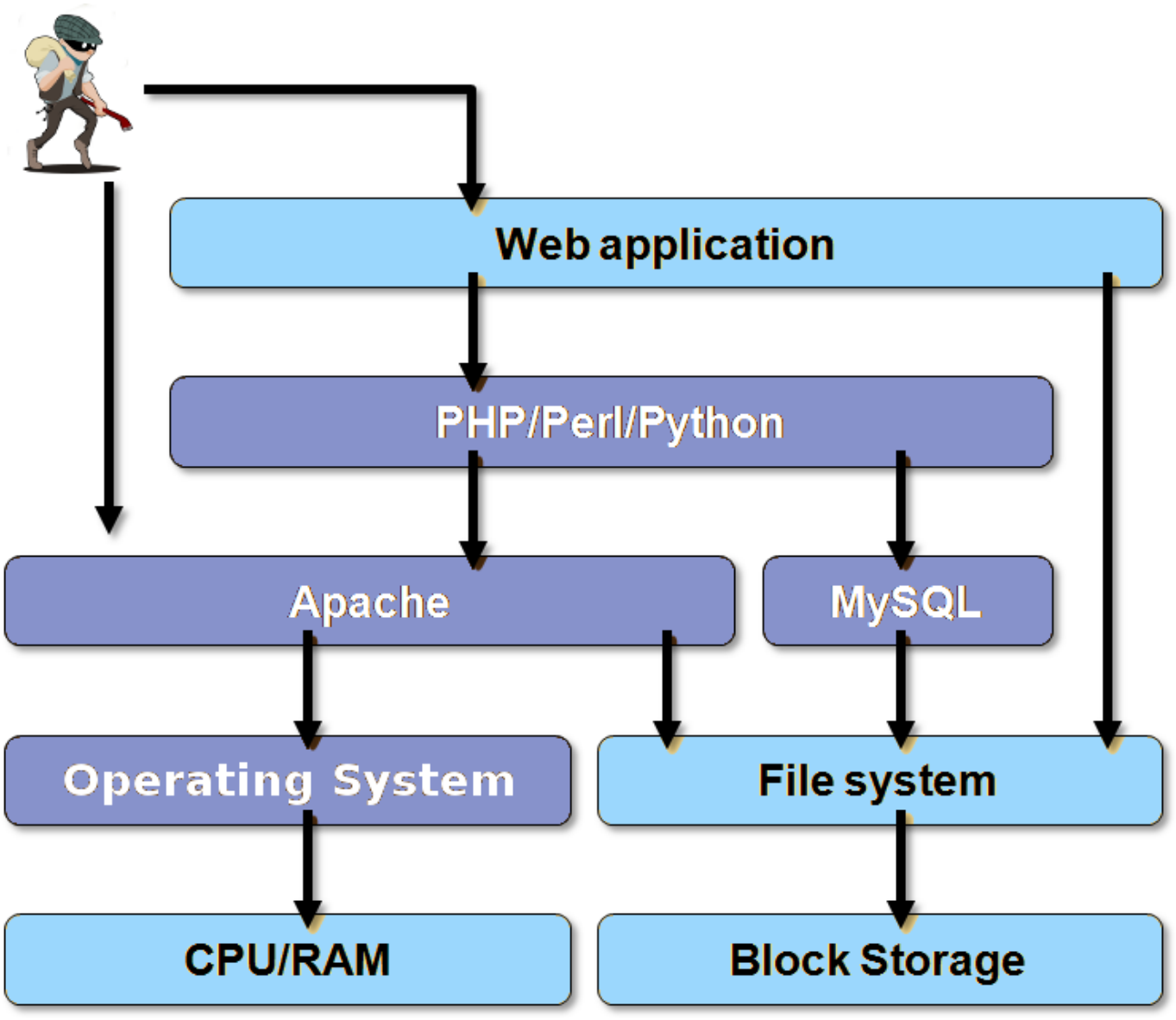
Some key changes that might need to be made are increasing the memory allowance and file uploads in PHP, or the file performance types and memory allowance in MySQL. These have to be matched with resources on the physical machine.

3.3 I can describe the way a web site functions

Learners should be able to describe how a web site functions in terms of the key components and how they interact

Additional information and guidance
Understanding how a web server works will help learners appreciate how it can be defended and from what. A web site, as understood here, is the software and hardware that allows someone to use resources on a computer in a destination. If the web site is for information, then anyone should be able to access that information when they need to. If the data on the system is for very specific people, then only those people should be allowed on.

Learners could make a simple diagram with call outs to explain how a web site works. They can use their own design as a guide as this will determine how the site functions and the purpose of various aspects of it. The following is an example.



At each point in the diagram some kind of breach could occur with different tools and for different reasons.

3.4 I can describe the main pieces of software required

Learners should be able to describe the software used

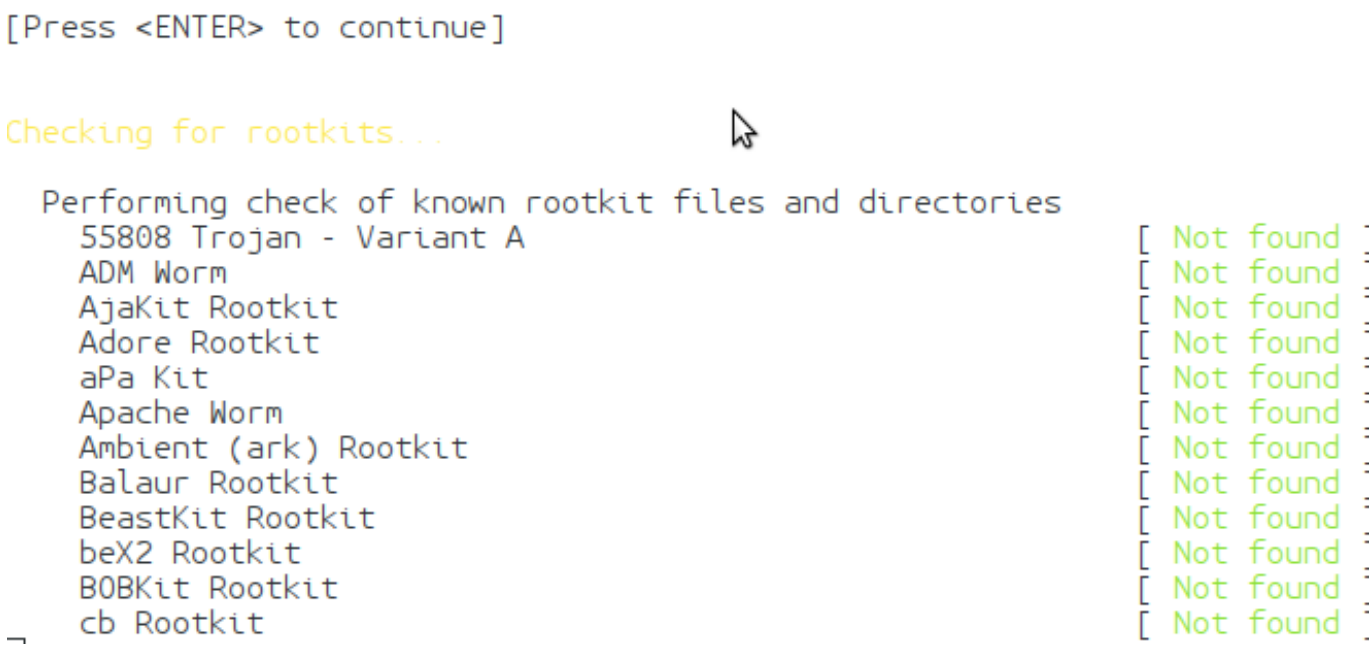
Additional information and guidance
It is likely that learners will have documented some elements of their system hardware in other units, but here they will describe them in terms of what they are doing for their system especially as it relates to security. They will probably be using LAMP as their core system, but what other software will they be using and for what reason.

Some other elements might include:

- Fail2ban http://www.fail2ban.org/wiki/index.php/Main_Page [2]
- Rootkit hunter http://rkhunter.sourceforge.net [3]
- Snort https://www.snort.org [4]
- Etherape http://etherape.sourceforge.net [5]
- Squid http://www.squid-cache.org [6]
- Spamassassin https://spamassassin.apache.org [7]
- Nmap https://nmap.org [8]
- IPTables http://www.netfilter.org [9]
- SuExec https://httpd.apache.org/docs/2.2/suexec.html [10]

Each of these can be used in different ways and will allow learners to protect their system and analyse any issues that might be occurring. Some of them might be part of an existing system, such as Linux, but may need configuring.

If rootkit hunter is set-up correctly, it will give detailed feedback on what types of attack are being prevented and if any have occurred since the last run. It could also be automated to run via a server cron job.

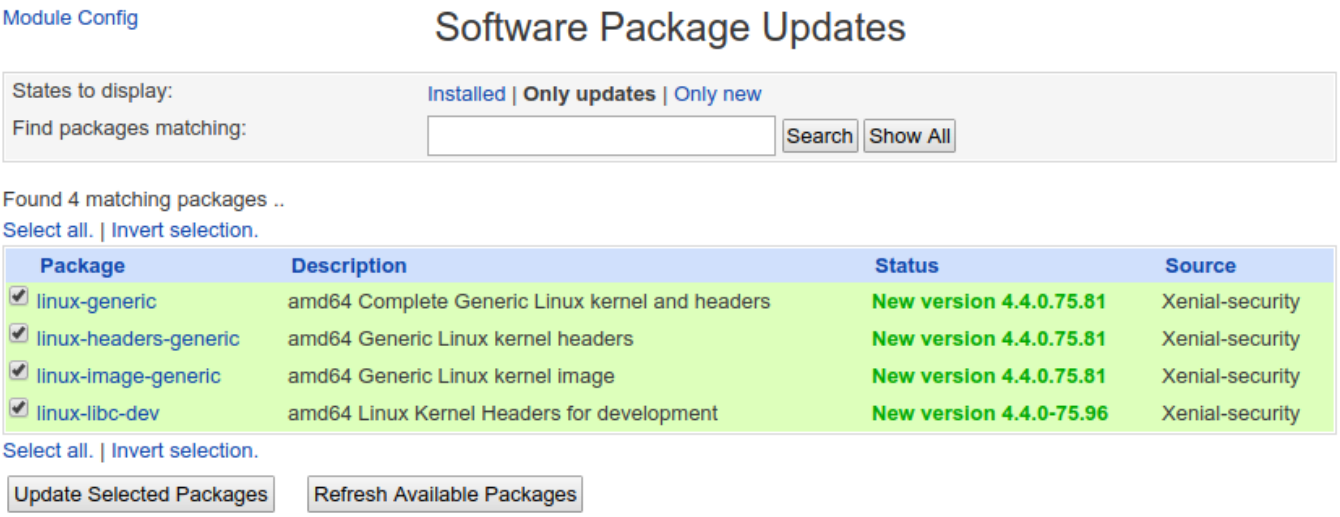


3.5 I can describe the configuration settings for a working system

Learners should be able to demonstrate the the main configuration settings

Additional information and guidance
Most of the key pieces of software will have their own configuration default settings, for example the Apache configuration file will specify which modules will be loaded and what directories will be served. In most cases, the default settings will be enough, but in terms of security, there will likely be additional settings for hardening the system. The most obvious one for Apache is to load and apply SSL connections to encrypt data to and from the server. There will also be additional configuration settings for php to make sure the security modules are loaded and that certain elements don't run, such as the open_basedir directive which prevents scripts from running other than in the specified locations. This prevents people placing executable files inside your web site as far as possible.

Another key aspect will be to maintain the overall integrity of system through fixes and patches created by the maintainers of the system, such as the particular distribution. The following screenshot shows a message from the management system that there is a security fix for the underlying kernel that needs to be applied.



3.6 I can recommend final adjustments before going live

Learners should be able to adjust the system in light of feedback

Additional information and guidance
In relation to the above criterion, if the settings made are not sufficient, such as with a web based system that uses a lot of memory, there may need to be additional adjustments. The following is an example that will appear on a site for MySQL and then PHP.

WARNING[23751]: res_config_mysql.c:1538 mysql_reconnect: MySQL
RealTime: Insufficient memory to allocate MySQL resource.
Fatal error: Uncaught exception 'ImagickException' with message 'Insufficient memory (case 4)

If these types of error, or similar, occur, learners need to understand enough to fix this going forward. In many cases, the site will not work as expected and will need to be fixed.

4.Test the system against common threats

4.1 I can develop a basic test regime

Learners should be able to create a workable test plan

Additional information and guidance
The type of tests required will be determined to some extent by the system used, for example a web

system designed just to display low value information will have very different requirements to a system which has very protected and valuable data.

The plan should work in a systematic way to make sure that all aspects of a site and all levels are protected. The two main ways that threats are generated are by push or pull methods.

- Push methods - SPAM, phishing, spoofs, malware, injections, pharmings, spear phishing
- Pull methods - ‘drive-bys’ to pull you from a legitimate site to a fake one to steal information.

Some of these methods can be instigated through seemingly safe methods such as email, while others, such as injections, will require the cyber criminals to gain access to a server. Each of these will require a different type of approach and in all cases both will need to be implemented.

4.2 I can explain the purpose of the main test procedures

Learners should be able to justify some of the tests used

Additional information and guidance
Some of the tests carried out might be obvious, such as blocking certain types of code from running on sites, while others may be less obvious such as disabling the ability to logon directly to the server as root. Many inexperienced people might set up a basic server for themselves using Linux as it is free to do, though many Linux systems by default allow SSH as root. It is easy enough to change this in a configuration file, but it requires the knowledge to know this is necessary. Similarly, the ssh config file can be changed so that the default port for ssh logins is not 22. The reason for this is that the default port of rssh is 22 so cyber criminals will automatically try this. By changing it to another number this can prevent or at least slow down attacks. Once this has been changed, the learners can then try to login as root and with port 22.

The purpose of these tests will then be along the lines of:

- Trying to access using ssh via port 22 to see if it is enabled.
- Trying to logon to a web server using the web address and directory to make sure it is not accessible

The learners should make clear why the tests are being performed and what they hope to deter or prevent.

4.3 I can explain the expected results from the test

Learners should be able to explain the outcomes that should occur

Additional information and guidance
Linked to the above criterion, the learners should have a clear idea of what should happen and can then look for any anomalies and fix them.

The following is some of the SPAM report from an email supposedly from Facebook, but it is easy to see the trail of servers it has com through and some of the purpose.

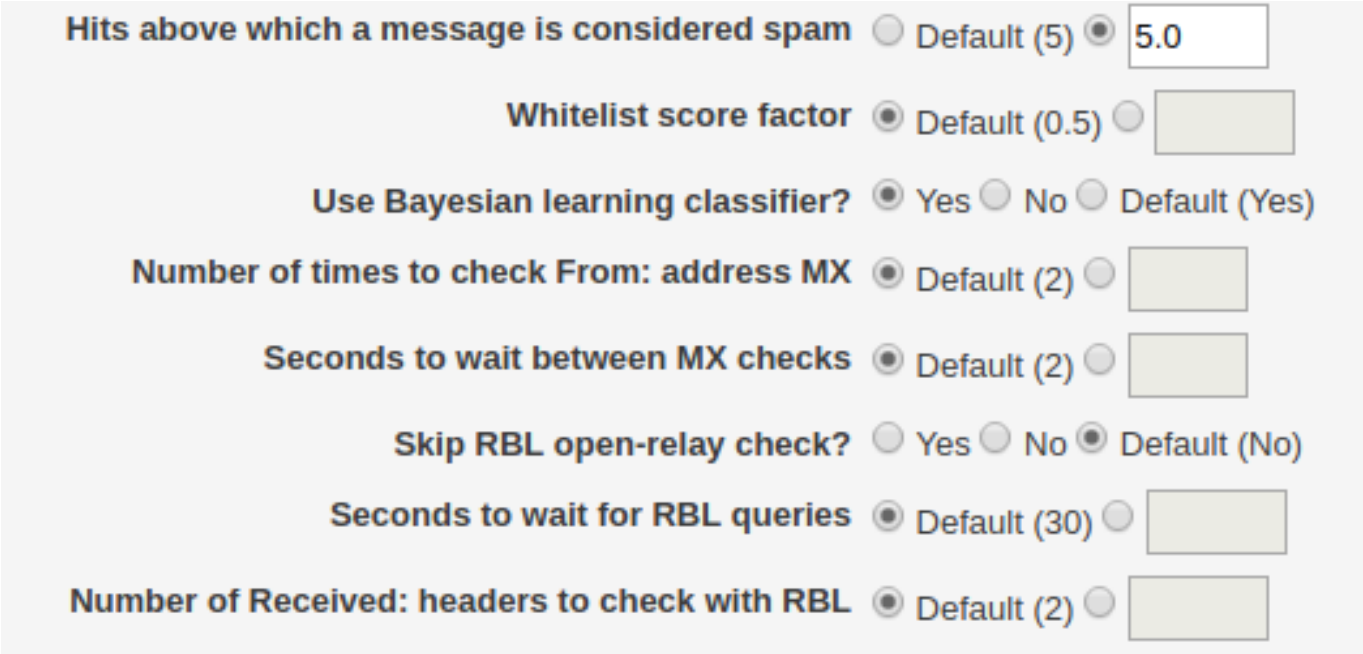
```
Content analysis details:   (24.1 points, 5.0 required)

 pts rule name              description
---- ---------------------- --------------------------------------------------
 1.2 URIBL_ABUSE_SURBL      Contains an URL listed in the ABUSE SURBL blocklist
                            [URIs: newtabsservices.ru]
 1.3 RCVD_IN_BL_SPAMCOP_NET RBL: Received via a relay in bl.spamcop.net
              [Blocked - see <http://www.spamcop.net/bl.shtml?212.71.255.188>]
 2.5 URIBL_DBL_SPAM         Contains a spam URL listed in the DBL blocklist
                            [URIs: newtabsservices.ru]
 2.7 RCVD_IN_PSBL           RBL: Received via a relay in PSBL
                            [212.71.255.188 listed in psbl.surriel.com]
 0.0 RCVD_IN_MSPIKE_L5      RBL: Very bad reputation (-5)
                            [212.71.255.188 listed in bl.mailspike.net]
 0.4 RCVD_IN_XBL            RBL: Received via a relay in Spamhaus XBL
                            [212.71.255.188 listed in zen.spamhaus.org]
 3.3 RCVD_IN_SBL_CSS        RBL: Received via a relay in Spamhaus SBL-CSS
 1.7 URIBL_BLACK            Contains an URL listed in the URIBL blacklist
                            [URIs: newtabsservices.ru]
 1.4 RCVD_IN_BRBL_LASTEXT   RBL: No description available.
                            [212.71.255.188 listed in bb.barracudacentral.org]
 0.5 RCVD_IN_SORBS_SPAM     RBL: SORBS: sender is a spam source
                            [212.71.255.188 listed in dnsbl.sorbs.net]
 0.1 URIBL_SBL_A            Contains URL's A record listed in the SBL blocklist
                            [URIs: newtabsservices.ru]
 1.6 URIBL_SBL              Contains an URL's NS IP listed in the SBL blocklist
                            [URIs: newtabsservices.ru]
```

It is clear to see from this a lot of the servers are listed on banned sites such as spamhaus and also that the main offender site seems to be newtabservices.ru, .ru being a server based in Russia.

4.4 I can describe the test results and what they mean

Learners should be able to describe some of the more important findings which demonstrate their understanding of the results

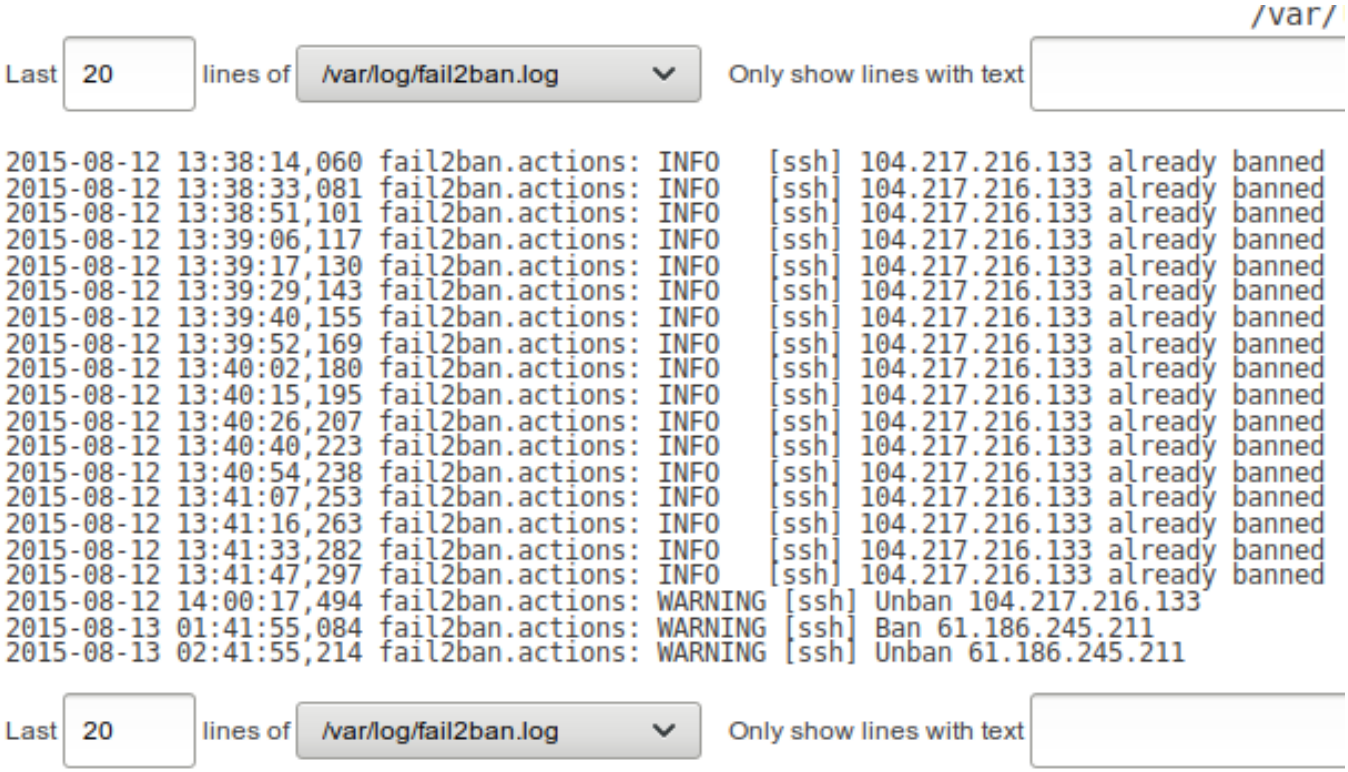
Additional information and guidance
In the above criterion, there are a number of details listed in the email logs, for example, that document some of the issues relating to the email. There are details about what type of checks were applied and basic details such as the level variance from the “norm”. In this case, an email with a score of 5.0 would be acceptable and the email above has a score of 24.1. Learners could explain how these points are calculated and how they can be adjusted and tuned. Is a score of 5.0 too low, too high, just right? How would you determine how the level is set. The following is a graphical menu to set spam levels and other actions.



Each of the reference sites in the email log shown in 4.3 will then be given a score and once it goes above 5.0 it will be labeled as spam.

If the client has an email client with a spam folder enabled, it will see this header and place the email into the spam folder or delete it.

Other logs should demonstrate similar settings, such as the access logs for ssh to make sure attackers are being banned as required.



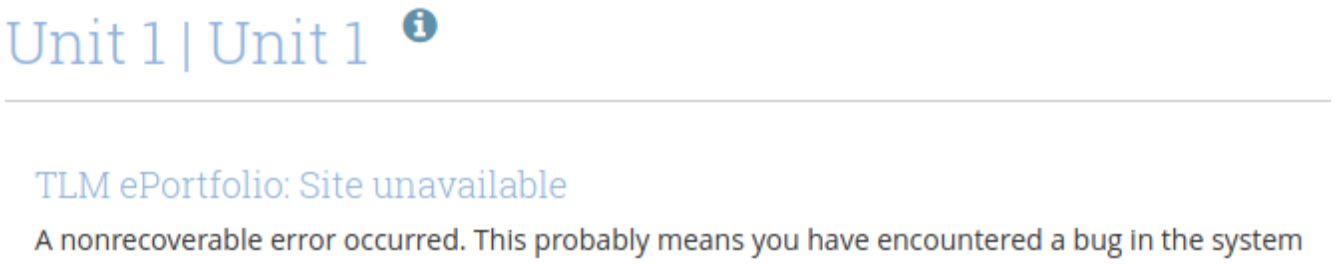
4.5 I can adjust the system in light of test results

Learners should be able to demonstrate they are able to act on information gained

Additional information and guidance

If a system is too aggressive in terms of labeling email as spam, it may need to be adjusted and re-checked until it works as required.

A web server needs to be secure, but in some cases it may be so secure as to not work properly and these error messages need to be adjusted. The following graphic is from a system that is supposed to allow users to create their own portfolio pages. The system required the web site it is running on the be able to write data into a temporary file to make the new pages. If the server path does not allow the web server to write to this folder, the page can not be created and an error message is then served.



The message is a generic one from the web based system and can be modified as required. There will also be a corresponding error message in the web server logs to try and fix the issue.

4.6 I can document the test results for third party support people

Learners should be able to create a document of their system tests so that a another person could re-create them

Additional information and guidance
Learners need to get into the habit that they may not always be the person working on this particular site and that someone else will need to know what they did and how. A key part of a security regime is the ability for it to be monitored and constantly checked. It may be that the learner gets moved to another project or leaves to join another company, or could be away on extended leave. In all these cases, someone else will be made responsible for the security of the system they set-up and they will need to be able to find information to maintain or improve the security.

Clear and concise documentation of all aspects of a system are very important.

5.Evaluate the effectiveness of the system

5.1 I can analyse the results in terms of the objectives

Learners should be able to evaluate their system against targets set in the planning stage

Additional information and guidance
How well did the system work compared to expectations? Was it as secure as it could be. Were the main attacks thwarted. These are some of the questions that can be asked and answered in evaluating the overall effectiveness of the system and the quality of the defenses enabled and configured.

Learners should write a brief set of comments with examples to show how well they have met their overall objectives for the system.

5.2 I can evaluate some of the features of the system and their purpose

Learners should be able to demonstrate an appreciation of why they use certain elements

Additional information and guidance
This criterion is an extension of other elements such as section 3 where they are explaining some of the features of the system. In this case, they go one step further to analyse what exactly works and why. How well designed are they and could they be improved. It might be useful to join one of the communities that look after some of the key pieces of software to see what kind of developments are planned. This will give them some insights into issues or limitations they may be experiencing and how they might be fixed.

5.3 I can justify some design decisions in terms of objectives

Learners should be able to explain the designs they deploy in order to meet some key objectives

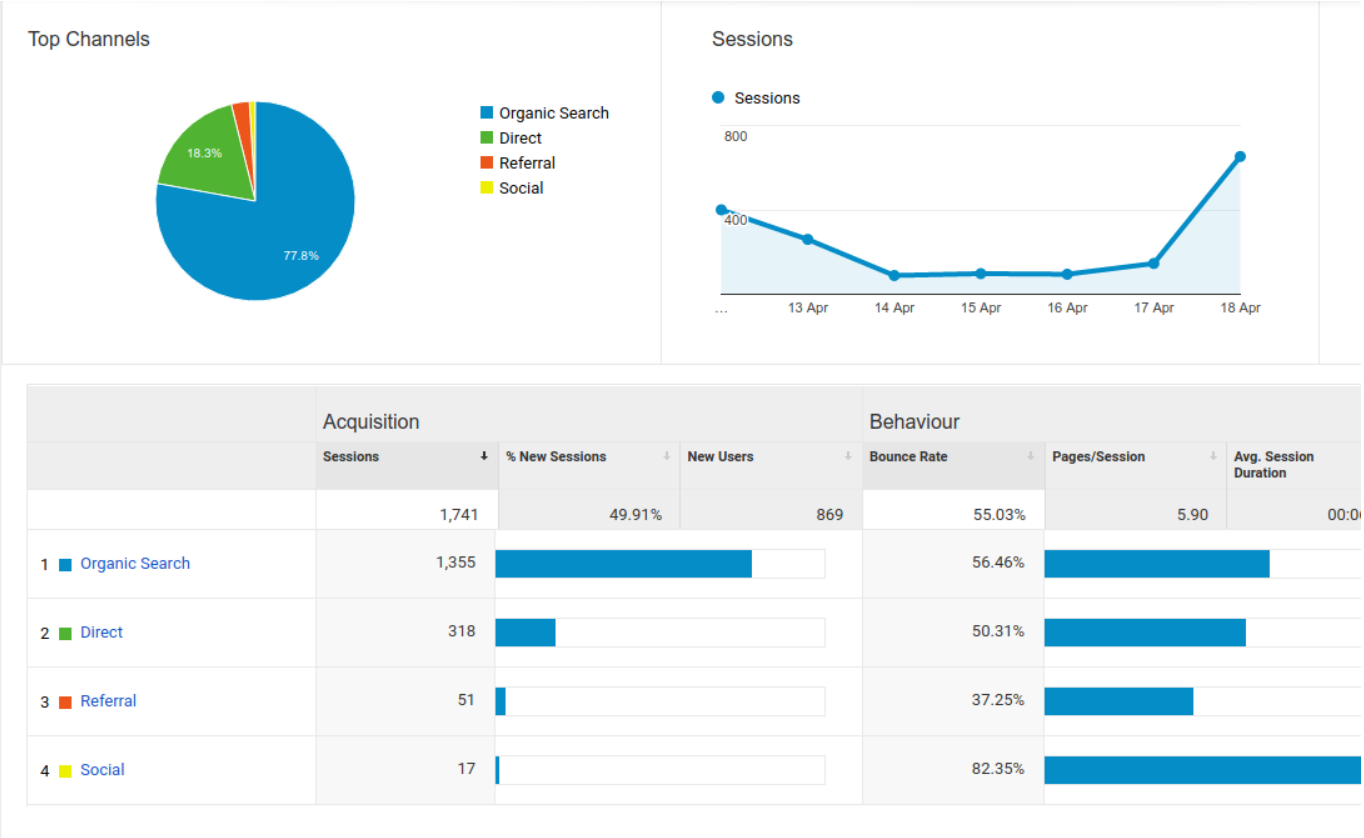
Additional information and guidance
In many cases, there will need to be some choices made in terms of reliability versus performance, or flexibility versus security. A very secure site might also be unusable, so there will need to be some design choices made for the best possible outcomes. These may be determined in advance if using a client who has specific needs as far as their end users, but could also be reflected in the skills and understanding of the learners. If they can justify having a slightly higher level of security that causes some issues for end users because of the limitation of certain threats, then this will need to be documented. The learners may have implemented a more
system of adding users so that their roles and permissions can be more tightly controlled. This might cause some level of inconvenience, but will make the system far more secure and if the expected numbers of users is quite low, this is a worthwhile compromise.

Some evidence of these sorts of value judgements needs to be clearly visible in some aspects of the design or in reflective journals.

5.4 I can analyse possible improvements to the system based on usage and end user feedback

Learners should be able to use logs and user feedback to make adjustments

Additional information and guidance
Most sites used will have some sort of feedback page or contacts link so that information can be gathered about how the system is working. Learners can also sign up for free analytical tools such as the tools provided by some of the bigger search providers like Google or Yahoo.



These tools allow you to check every aspect of your website in terms of who comes to the site and what they do, how much data is sent and received and even if people click from the site to other sites or come to the site from other sites. This data is invaluable in determining how effective a site is in terms of the overall purpose.

It should also alert the designer to where the most traffic is coming from and if the traffic is from sites or regions known to cause disruption or hacking they can take some evasive measures.

Other tools have been mentioned elsewhere in this guide.

5.5 I can analyse the effectiveness of the system by viewing the different log files

Learners should be able to gage the effectiveness of their actions by the reduction of attack numbers

Additional information and guidance
The log files will act as a guide as to how many attacks are occurring and from where. On a small site, the numbers might be quite low anyway as most sites are attacked for their potential of returns and a small traffic site may not attract enough attention to warrant an attack. Having said that, most learners will be aware that as soon as they switch on a broadband connection there is a flood of attacks from automated devices.

This criterion could be validated quantitatively, such as saying that before their actions there were e.g. 100 attacks a day, and now there are just 10, which would be a 90% reduction. They could also use qualitative measures, e.g. there are less attempts at SSH attacks as I have secured the port and stopped root logins.

Screenshots or videos would be useful as reference.

5.6 I can recommend improvements to the system for future- proofing

Learners should be able to demonstrate some level of appreciation of future developments

Additional information and guidance

(function(i,s,o,g,r,a,m){i['GoogleAnalyticsObject']=r;i[r]=i[r]||function(){ (i[r].q=i[r].q||[]).push(arguments)},i[r].l=1*new Date();a=s.createElement(o), m=s.getElementsByTagName(o)[0];a.async=1;a.src=g;m.parentNode.insertBefore(a,m) })(window,document,'script','//www.google-analytics.com/analytics.js','ga'); ga('create', 'UA-46896377-2', 'auto'); ga('send', 'pageview');

At this level it is not expected that learners become experts in the field, but their research and practice should be such that it gives them some ideas about what else can be done. It may be that they feel the need for a more robust connection to the Internet for their system and they may recommend, for example, that the basic router provided by the ISP be upgraded to a newer and more feature rich version. They may feel there is a need for a heavy duty hardware firewall to be put in place.

Other such recommendations should be clearly described.

Links
[1] https://en.wikipedia.org/wiki/LAMP_%28software_bundle%29#/media/File:LAMP_software_bundle.svg
[2] http://www.fail2ban.org/wiki/index.php/Main_Page
[3] http://rkhunter.sourceforge.net
[4] https://www.snort.org
[5] http://etherape.sourceforge.net
[6] http://www.squid-cache.org
[7] https://spamassassin.apache.org
[8] https://nmap.org
[9] http://www.netfilter.org
[10] https://httpd.apache.org/docs/2.2/suexec.html