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

Overview

The candidate can plan and review their use of commonly used security tools to demonstrate some of their skills and understanding. They will investigate and try out some of the more commonly used and recommended security tools and services. They will use this understanding to consider some of the ways that attacks are carried out. They will practice recommended security processes and procedures to carry out investigations into attacks or to determine what might be attacked and document some of their thoughts and findings. They will evaluate the various tools and make some informed recommendations themselves based on ease of use and overall effectiveness. Throughout, they will consider the place of laws and legal protections in cyber defence.

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

Example of context – setting up a secure web site using something like Wordpress for a local organisation.

Assessor's guide to interpreting the criteria

General Information

RQF general description for Level 2 qualifications

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

Requirements

- Standards must be confirmed by a trained Gold Level Assessor or higher.
- Assessors must at a minimum record assessment judgements as entries in the on-line mark book on the INGOTs.org certification site.
- The work in the unit is recommended in order for candidates to have covered enough depth and breadth in the topic to successfully carry out their controlled assessment and take the external exam.
- When the candidate has covered as much of ths material as necessary to complete the controlled assessment element, they may be introduced to the topic
- This unit should take an average level 2 learner 35 hours of work to complete.

Assessment Method

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

Expansion of the assessment criteria

1.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:

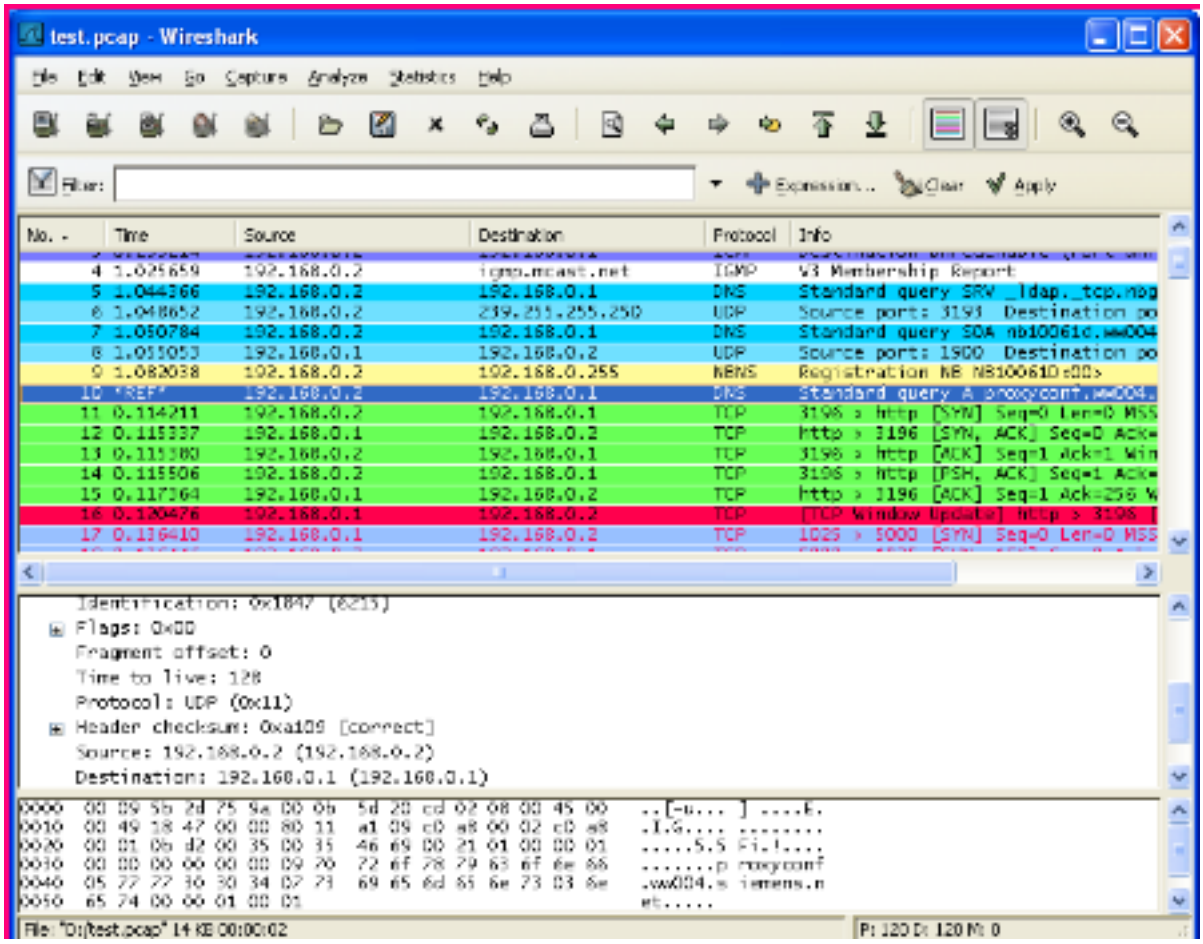
1. Vulnerability Scanners
One system already mentioned in this handbook is nmap (Network Mapper) which allows you to audit a network for any services running that could cause problems. Running a quick scan on your server should let you know if there are ports open that should not be and a decision can 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 however has seen great adoption amongst forensic analysts due to the power of its search function.

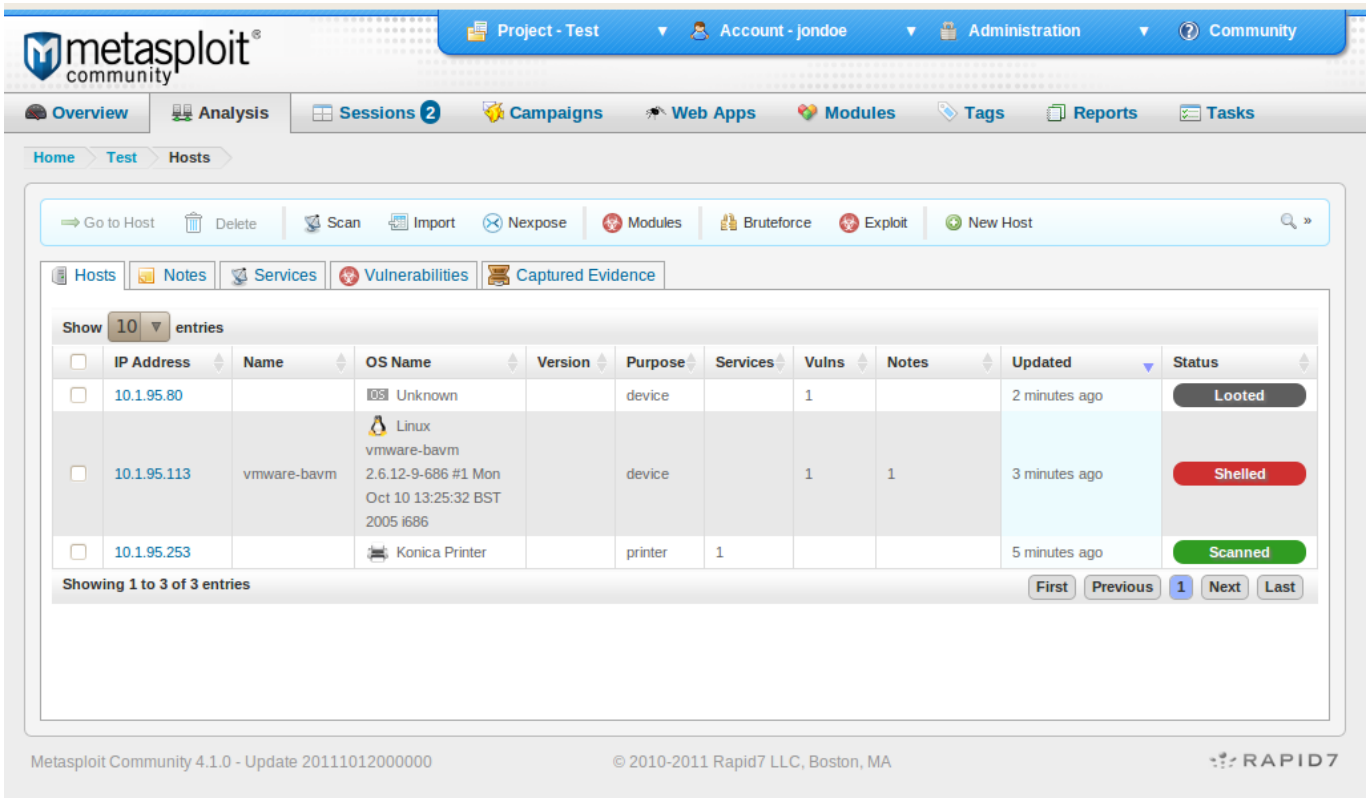


A third category of tools are those which are inbuilt in an operating system. Example the Task Manager in Windows or the similar PS Aux command in Linux lists running processes. While this is

useful in general computing for killing a process which has frozen they have roles in forensics such as identifying a malicious process which has infected a machine.

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.

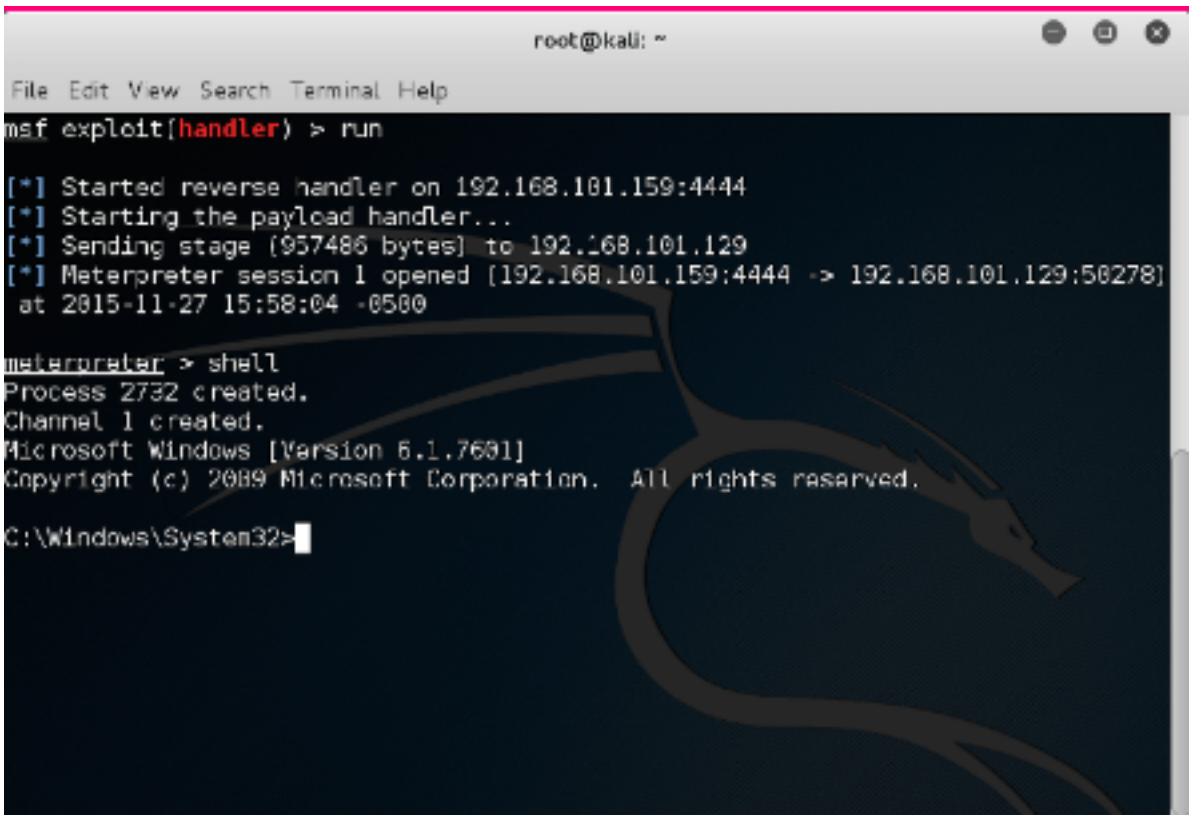


https://en.wikipedia.org/w/index.php?curid=33606448 [1]

The screenshot here shows that two of the computers have been exploited already.

The above picture is the windows version of Metasploit.

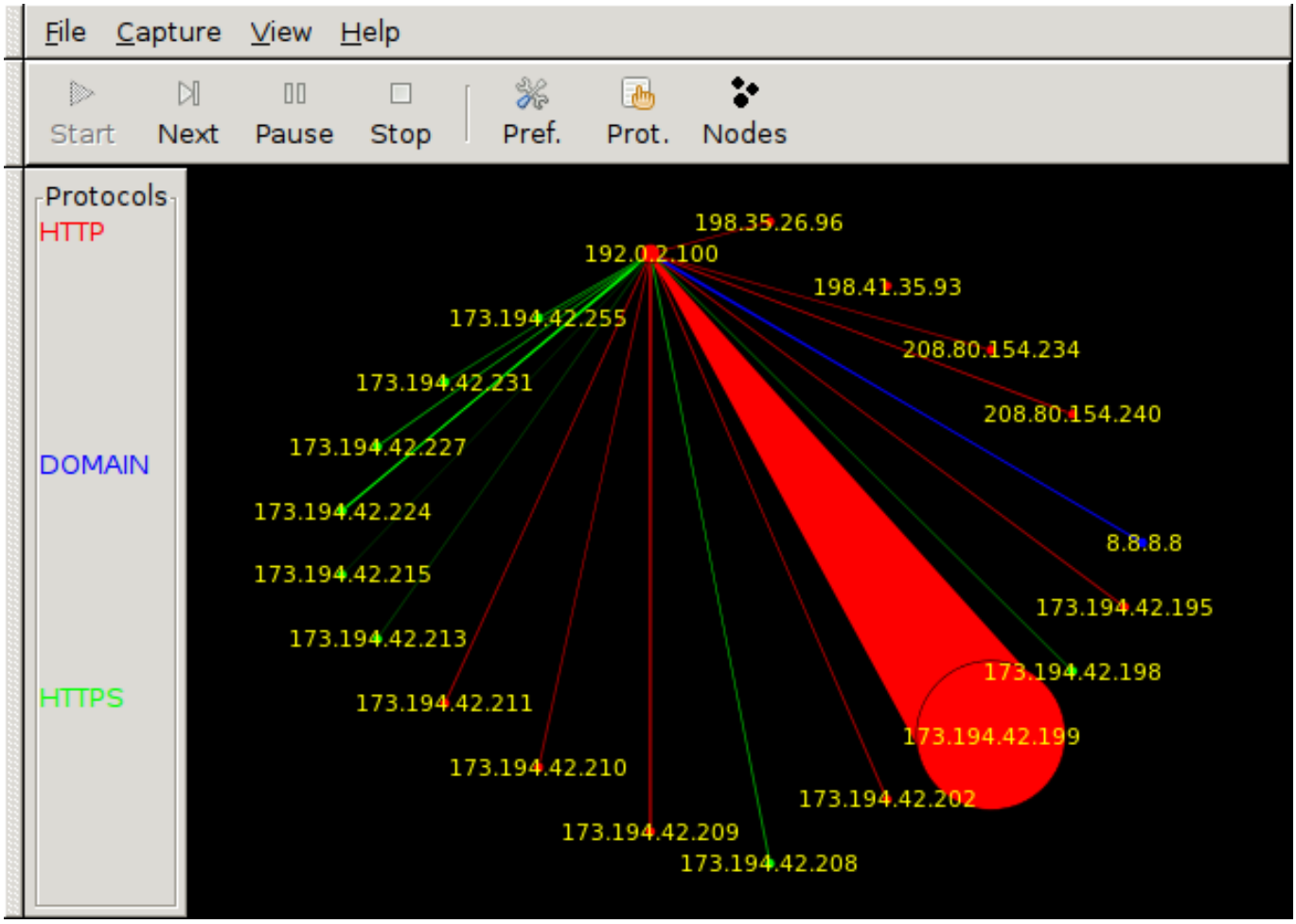
NOTE - Metasploit is the most dangerous program which will be mentioned in this course. It is impossible to avoid mentioning it. However great care should be taken not to encourage its use to a great extent. It may be appropriate to use Metasploit in a very limited way when looking at server security.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



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.

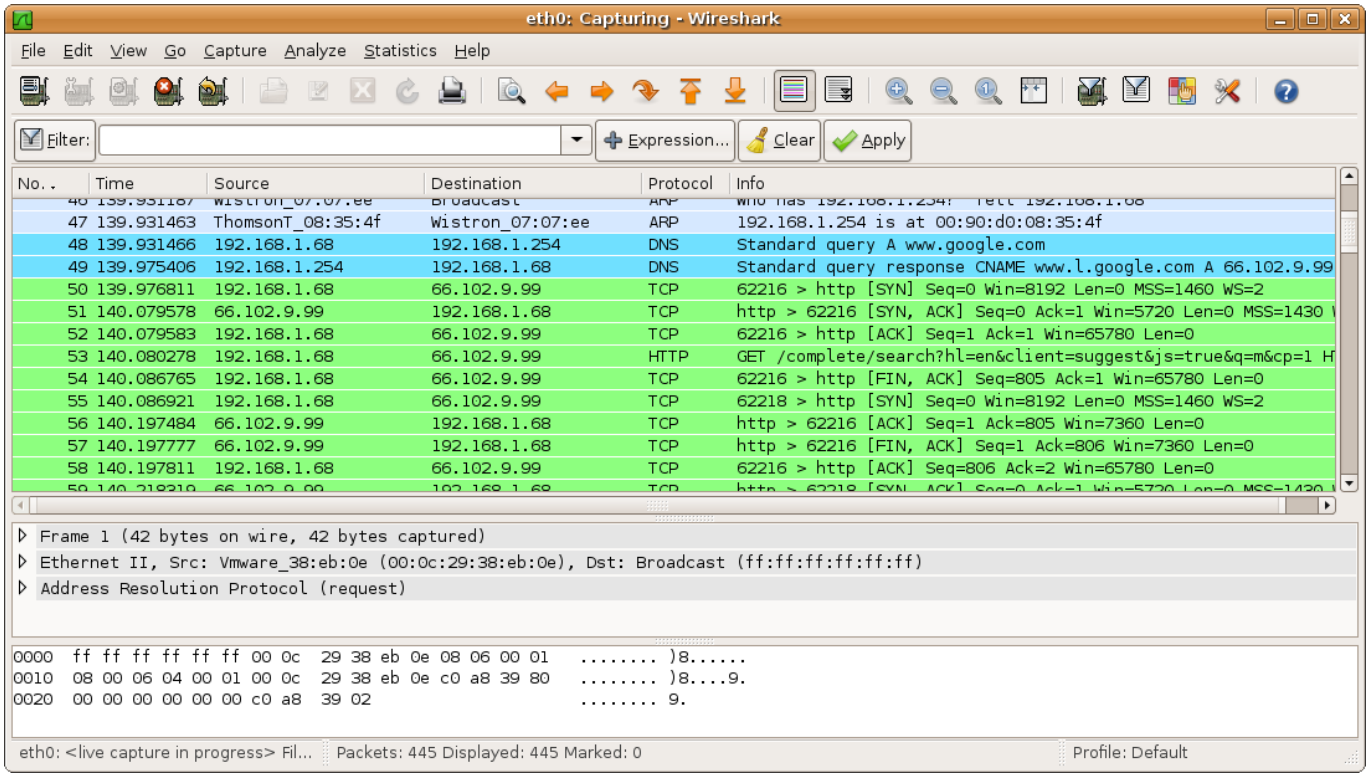
4. Network and Traffic Analyser
These tools are used to see what sort of traffic is coming in and out of a system to check if it should be and what can be done if there is a problem. There are a number of popular tools such as Etherape and Wireshark.

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



https://commons.wikimedia.org/w/index.php?curid=42671374 [2]

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



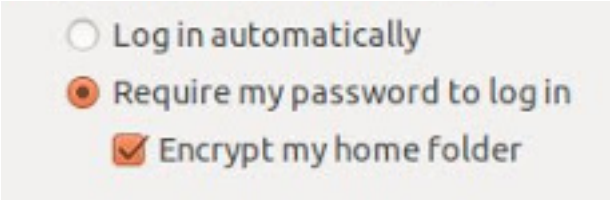
https://commons.wikimedia.org/w/index.php?curid=4042536 [3]

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 WiFi 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 a 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.

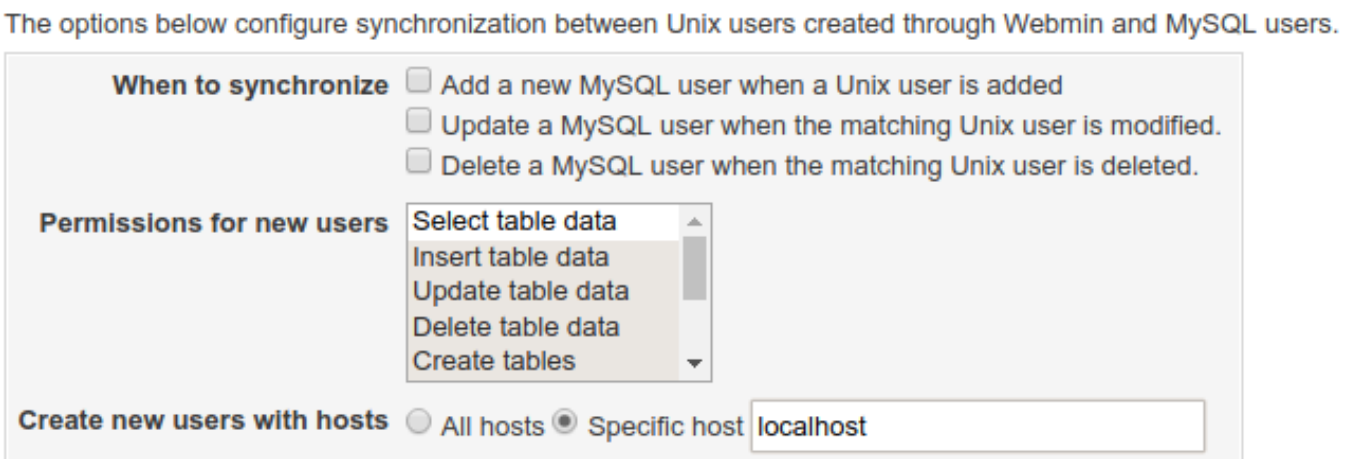
Additional information and guidance
Evidence here will depend on what investigations learners are carrying out. If they have access to local firms that deal in financial services, the tools used to protect data may be far more comprehensive that if they are dealing with a local organisation that does 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 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

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

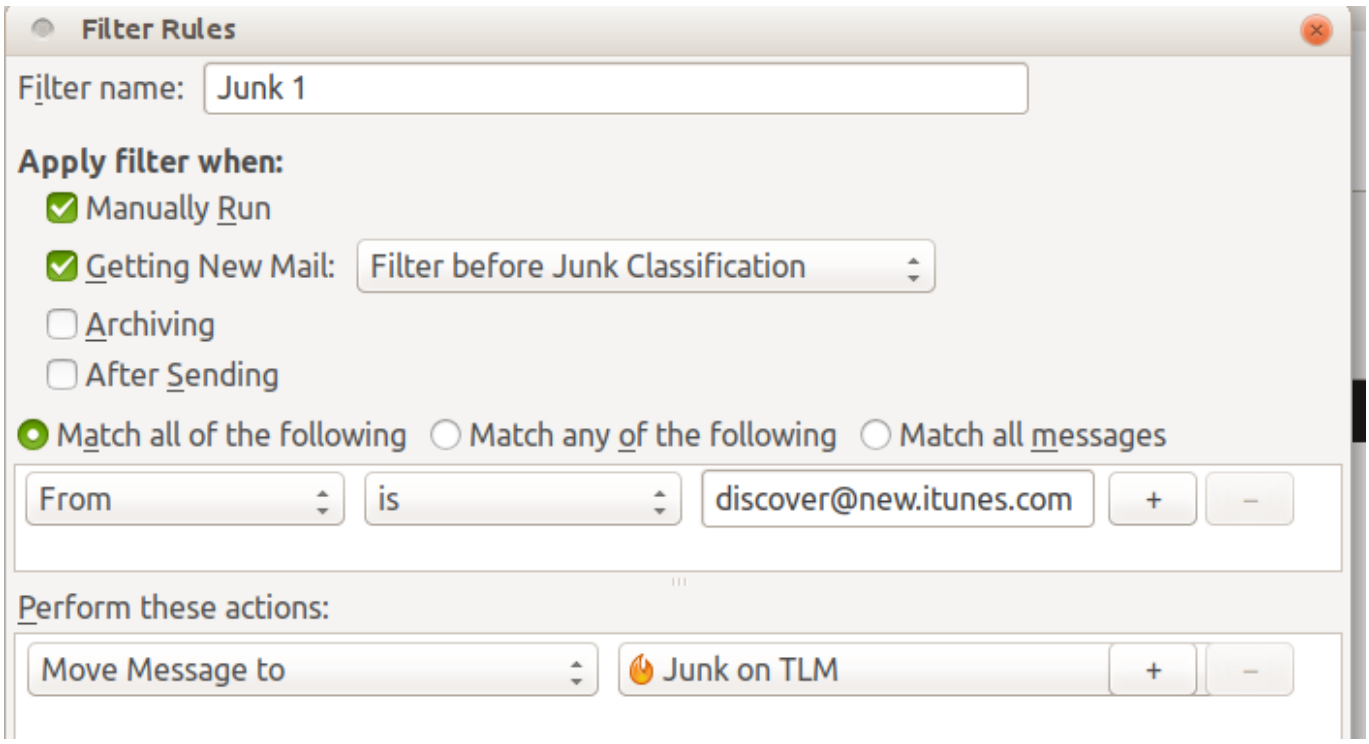
outside, such as web folders, they can create specific permissions to only allow reading and even create protected folders that can only be accessed with prior passwords. Many web server folders can have special hidden files that only allow specific access. On databases, users can set permissions on who can access the data and from what computer which helps with security.



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 **Iliketlm123** 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 [4].

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 25 th 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 €20,000 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.

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 there are three examples of an Nmap being run with three different levels of ability.

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 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 your 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 and 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.

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

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 as 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 that 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 or against the act.

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 anti-malware 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 can not 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 [5]

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 the seup 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 an 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.

Links

[1] https://en.wikipedia.org/w/index.php?curid=33606448
[2] https://commons.wikimedia.org/w/index.php?curid=42671374
[3] https://commons.wikimedia.org/w/index.php?curid=4042536
[4] http://openpgp.org
[5] http://www.bbc.co.uk/programmes/b08qgbc3