Unit 2 - Digital Safety and Security Policies and Procedures

Overview

The candidate can understand online threats are created and deployed and how much damage thy cause to individuals and organisations. They will investigate how to minimise these threats and document their processes to help others.

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

Example of context – what sort of routines and practices can be used to make sure that important files and media are protected, either on devices like USB sticks or online.

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 30 hours of work to complete.

Assessment Method

Controlled assessment and external examination.

Expansion of the assessment criteria

1. Understand the range and scope of threats and countermeasures

Learners will research and explore some of the threats to data and also some of the ways to stop or at least minimise these. This will give them a good grounding when working on projects and appreciating that they need to be made secure from the start, rather than later when it might be too late.

1.1 I can list the main threats to online safety

Learners will give an overview of the most common threats

Additional information and guidance

Learners will create a list or table of some of the more common threats associated with using technology. In many cases, they will have experienced some of these first hand, such as phishing or Pharming, where someone sends them a realistic and believable email from a company and asks them to login and to a website or send their details back. Other common threats will be:

- Fraud and financial crime

- Terrorist related

- Extortion

- Warfare

- Viruses/malware

- Denial of Service

- Spam, phishing etc

- Obscenity
- Harassment/trolling/bullying
- Trafficking

Some of these threats, like SPAM, are generally just annoying, but harassment and bullying are very serious and cause a great deal of harm and long term damage.

Does the nature of the threat determine the nature and seriousness of the countermeasure?

1.2 I can list the main ways to minimise online threats

Learners will be able to show some research results into ways to stop some of the above listed threats

Additional information and guidance

Learners should be able to document and briefly describe or detail the main features of some common means to counter online threats. It is likely they have had some kind of school or college based sessions on how to deal with some online problems and at home they will likely have investigated ways to protect their home system. In this instance, they will just need to collate some of their findings, perhaps as a table. They could combine all their research into one table.

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

1.3 I can explain the damage threats done to individuals

Learners will begin to explore some of the threats from different angles.

Additional information and guidance

Learners will have shown some of the threats in basic terms previously, but can now explain in more

depth what damage is cause with some examples. As already mentioned, there is a huge increase in online harassment as a result of so many young people now having constant access to them through mobile devices. There has been a significant increase in mental health issues in recent years. Other personal level problems will result from fraud. Many elderly people have been targeted since they were allowed access to their pensions before a certain age. This meant that people would phone them pretending to be from pension companies or investment companies and convince them to divulge their bank details, so losing all of their savings.

Perhaps learners have friends or families that have been attacked in some way via online threats.

1.4 I can explain the damage threats cause to organisations

Learners will research and explain what damage is caused by threats to organisations

Additional information and guidance

Learners will have shown some of the threats in basic terms previously, but can now explain in more depth what damage is cause with some examples. For example, if discussing financial damage, the attack on TalkTalk in 2016 is estimated to have cost the company £60 million. None of this was direct damage but was fines from the government and loss of customers as they no longer had confidence in the company to keep their data safe.

1.5 I can describe the methods used to counter threats with software

Learners will describe the software applications they use

Additional information and guidance

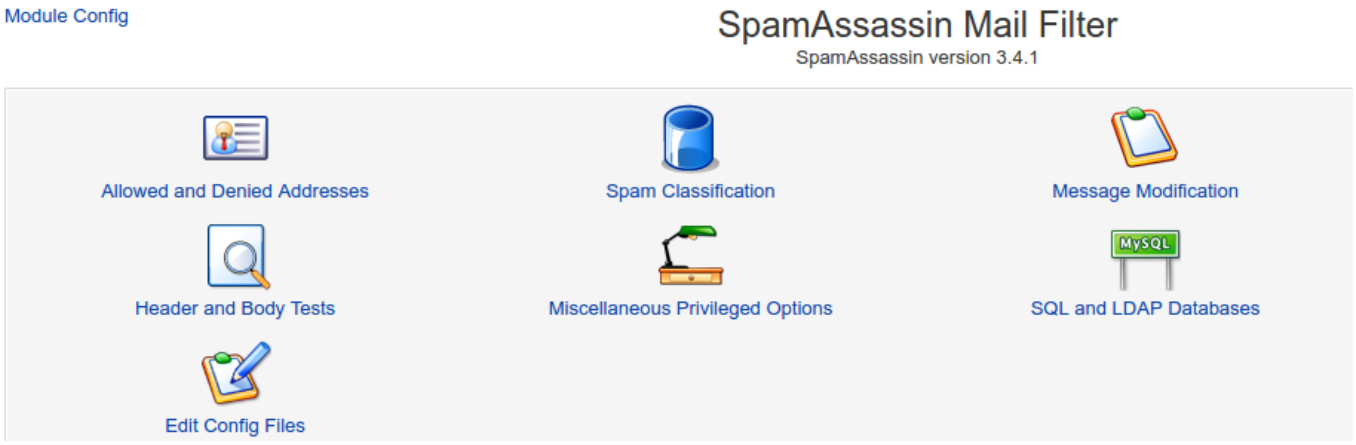
In most cases, students will talk about personal protection systems as they may not have access to server based systems, though the centre could organise a talk with the IT team to go through what is carried out. Most software they will be familiar with will be anti-virus software, which usually incorporates anti phishing as well as applications to minimise attacks. Learners need to pick a package or a number of applications and describe what features they offer. The popular open source antivirus software ClamAV carries out a number of functions.

http://www.clamav.net/downloads [1]

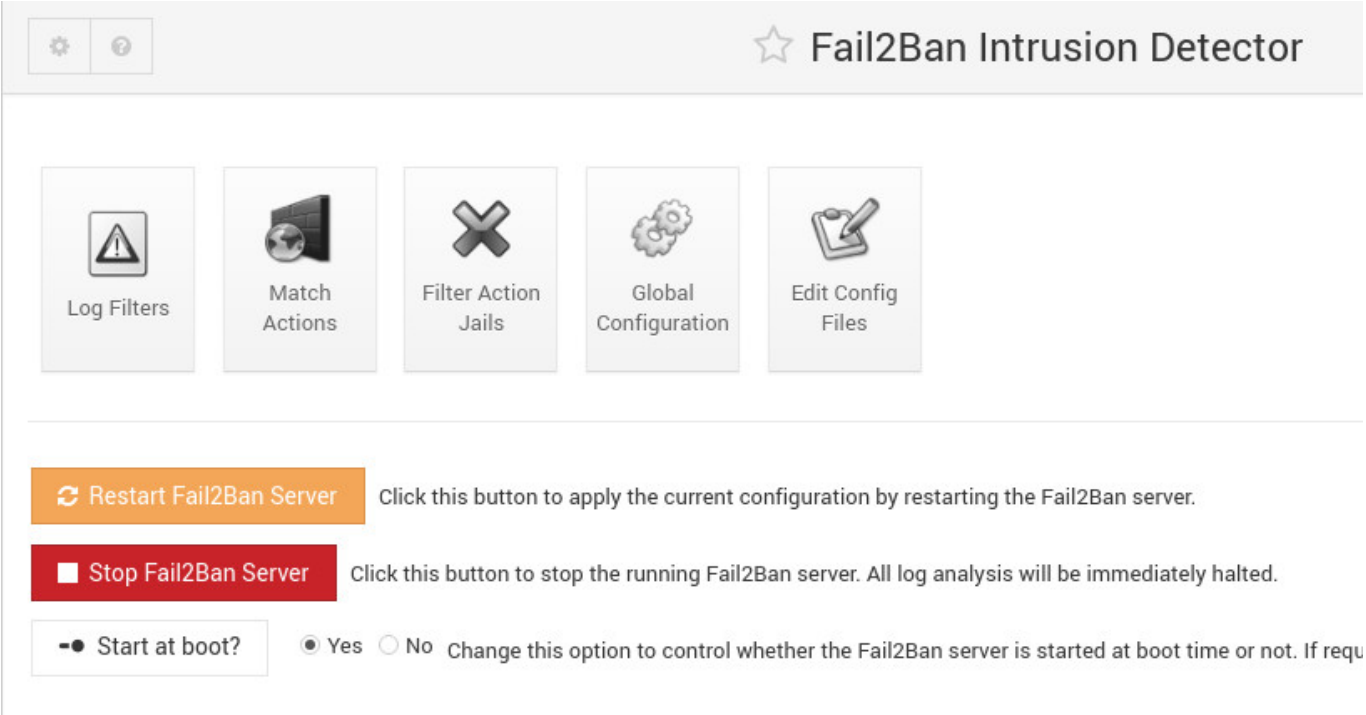
It also, like many others, updates it’s antivirus database regularly so that new “signatures” of viruses and malware can be detected and removed. For windows, there is a GUI version from Immunet. The system uses the cloud to look for new viruses and add them to the local database when scanning.

At the server level, especially in relation to the Internet which is about 80% dominated by Unix based machines, there doesn't tend to be many GUI based system, but there are web based management tools such as Webmin that give access to antivirus and protection tools.

There are tools such as Spamassassin for checking email for spam and marking it as spam.



Or Fail2ban to stop people trying to login to a server.



Learners can research and describe as many tools as they feel they need to to get a good understanding of the options.

1.6 I can describe the methods I use to protect myself online

Learners should be able to describe their own practices for protection

Additional information and guidance

The examples and descriptions will vary, depending on what learners use and how they deal with security. Most will be aware of centre based policies and AUPs, which they may adopt for their own needs. They should be able to describe a number of examples they use, for example, what settings do they use on social media and why. What actions do they take online when they are unsure of the material they are seeing and required to click on, such as emails or requests from others. How do they deal with putting images and thoughts online, knowing that these will never be deleted and can be shared, as has been shown by numerous examples in the press, with others even though privacy is supposed to be maintained.

In their descriptions, they can perhaps reflect on how important, or not, this is to them as online users. This sort of reflection is useful in guiding what they do and how they advise others once they have to do it professionally.

2. Apply a range of systems and services to deal with threat

Once they have investigated and understood the scope of threats and countermeasures, they can then show what they can do to deal with them.

2.1 I can explain the way threat are created and deployed

Learners need to research and explain some of the ways threats come about and get to users

Additional information and guidance

Learners will not need to spend too much time looking at online news services to get some examples of the multitude of threats occurring online and to get a sense of how they are made and how they get to people or organisations. They should understand that some threats are carried out by

organisations on organisations and some by individuals on individuals. As with everything, it depends on the value of the attack. In the news as this is being made, a company that creates Bitcoins has been attacked and 4,000 of their Bitcoins have been stolen. At the moment, this amounts to $80,000,000, so was carried out by a large organisation of dedicated hackers. Many individuals are attacked by smaller operators or individuals. It is assumed that 10% of people will be convinced by advertising or similar, so most hackers will probably work on this basis and assume that 10% of people they try to trick out of money or other goods will respond. This is enough to make them want to do it as 10% of 1,000,000 people will make them rich.

Many threats are created because systems are not well made. One of the strengths of Windows was that it was widely adopted and made to be as easy to use as possible, but this also meant it had inherent weaknesses, especially as it was designed before the Internet so not designed with this in mind. This has meant that over the years it has been relatively easy to find problems with Windows machines and since many people still use old and unsupported versions of Windows (look at the NHS Wannacry attack in 2017). Many people do not know how or in some cases don't care about updates and patches so their machines become easy targets.

https://answers.microsoft.com/en-us/windows/forum/windows_10-security/wanna-cry-ransomware/5afdb045-8f36-4f55-a992-53398d21ed07?auth=1 [2]

People’s computers may not be attacked to take their money, but may be used collectively as DDoS farms or devices to make attacks on systems that appear to come from them and not the actual hackers.

Learners need to detail some examples like this to show their understanding.

2.2 I can explain the hardware tools used to counter threats

Learners need to explain some hardware tools for security.

Additional information and guidance

Learners will most likely be familiar with the facilities of their home router which will offer many tools to assist them in protecting their privacy. The most important part of a router is the firewall. This is technically software, but since it is running on the router, it is more of a hardware solution. The firewall is a means of stopping external machines accessing internal networks. All computers carry out communication, in and out, via software based ports or doors. Some of these ports or doors need to be open. For example, if your computer sends email, it will usually use port 25 to send the email to other systems. This is the port used by the email send service SMTP (Send Mail Transport Protocol). Secure email can go through other ports such as 465. If you send files to another computer, your computer will use port 21. When you access a normal website, you are connecting to another computer on port 80 in order to download their files (the website). The purpose of a firewall is to close the ports that you don’t need, that others could try to use to get in, and monitor the ports you need so that you can use the Internet. If you want to run your own server on your internal network such as a game server, then you would need to give the outside world access to this machine. This could be done by using a router’s facility for using a DMZ (Demilitarised Zone). This makes an internal computer appear on the outside. If this is done, you would need to set up the DMZ computer to only allow safe services.

Other things you could discuss are the use of encryption for Wi-Fi devices and static IP addresses for home machines, linked to their MAC or machine address. There is also the use of VPNs (Virtual Private Networks) to make sure only you are accessing your network.

Learners can discuss other tactics and tools

2.3 I can explain the software tools used to counter threats

Learners can explain a range of tools they might use

Additional information and guidance

Many of the software tools will be applications on individual machines, rather than the infrastructure elements mentioned in the previous criterion. There is some overlap and there is no reason why you can't run a firewall on your router and on your individual machines.

The software will be things such as:

- Anti virus software suites
- Password managers
- Hard drive encryption
- PGP for email
- IP blockers
- Anti snooping checks
- Scans

There are many other software tools that can be explained and will depend on what individual learners have as a setup at home.

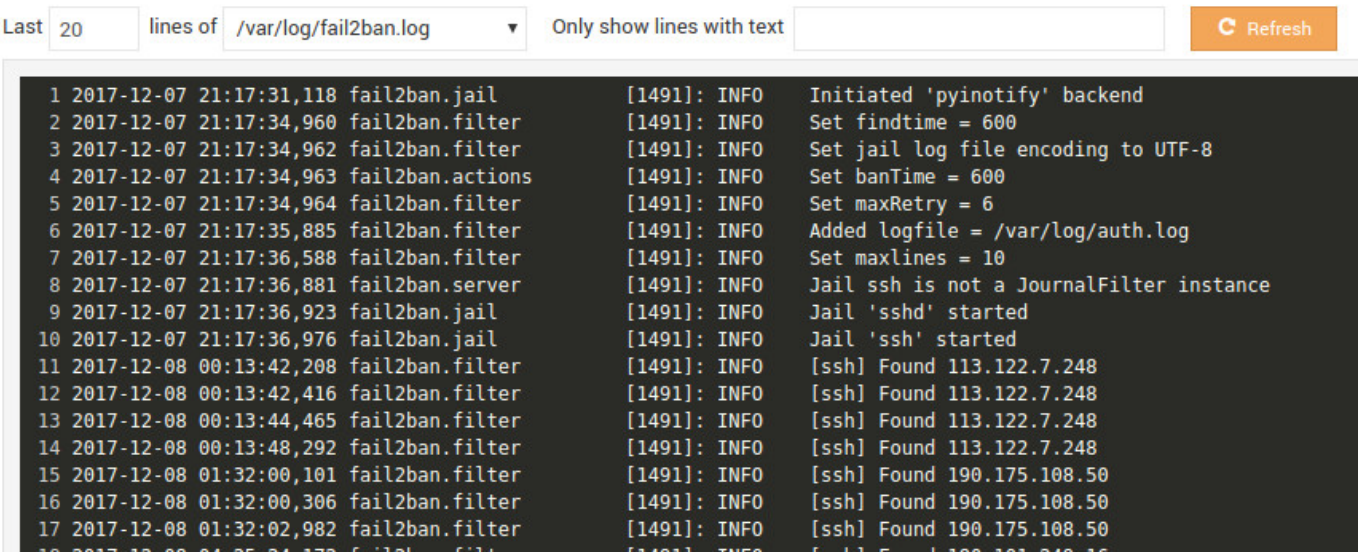
2.4 I can describe the way these tools minimise damage

Learners will go into detail about how these tools work, with examples where possible

Additional information and guidance

Depending on what they use, and without compromising their own security, learners can give some examples of how their systems protect their network systems. They can show some logs from their router which show what traffic is block or intercepted. They can show any virus software that is detected and quarantined by their software suites.

The following image is the log files from a DMZ computer running Fail2Ban software. The software blocks computers from outside based on their IP and after 4 attempts it will lock their address. This is usually enough for the hackers to give up and move on to someone else's computer that is easier to get into.



2.5 I can setup tools and services to protect a system

Learners should be able to demonstrate that they can apply their knowledge and understanding

Additional information and guidance

Learners can submit a video if it is easier than doing some screenshots and might be able to do some of this as a class if that is possible. They should be able to show some basic setup activities of setting up software applications. As with most of these elements, it will vary per user as some will have more access than others, but some basic setup is required to show they have a practical understanding and can then evaluate what works in the later parts of this unit. They might be able to point out some of the key settings they used and why they chose them or why the default settings were enough for their needs.

For services, some students could explain the security and protection services they use for some of their social media and show hat settings they use and why.

2.6 I can test the effectiveness of this system

Learners will show some results of their activities

Additional information and guidance

Most systems will have logs, though they may not always be switched on. This should give learners an idea of the effectiveness of their actions. If they make some changes to their filter system, does it stop more SPAM, if so, can they show how much difference it makes. Can they see how much traffic they get attacking their home Wi-Fi and then change the SSID or hide the network and see if it reduces the attacks. Are there some settings on their home router which make a difference to how much traffic tries to get in. Can they enable and set up some anti spam software on their email client. How much difference does it make to how much spam gets through.

In cases where it is difficult to test the system, or at least show some results, it may be advisable for a centre to ask the IT team to show them some of their systems and how they deal with attacks.

3. Evaluate and document policies and procedures to counter threats and increase safety

3.1 I can create a guide to the main threats

Learners will create a simple guide to summarise their knowledge and understanding

Additional information and guidance

As learners research and make notes on this topic, they will hopefully start to make some informed choices about what they can use and why. Depending on their client and what area they are focusing on, they will be able to put together a simple guide, or presentation, to show the main threats to the system they are attempting to defend. A short user guide will clearly show the extent of their knowledge and understanding and provide a clear way for them to keep track of what they are trying to manage. It would also be useful to get into the practice of documenting their efforts as professionally this is what would be expected of them.

Obviously, it will depend on the sensitivity of what they are doing, but they could do a screen recording or video of what they are working on if they prefer this medium and this will be useful for applications at a later date as it will clearly show their skills. They could incorporate this into their skills ePortfolio which TLM provide: https://eportfolio.tlm.org.uk [3].

3.2 I can produce a list of equipment to be used to protect systems

Learners need to document some of the equipment they have investigating

Additional information and guidance

A basic list or a table will be good for this criterion, though it is always useful to put in more detail if that is possible. The following criterion is going into more detail about the equipment, so these two may well be merged together. Learners can keep them separate if they prefer.

As with many things, the detail will be dependent on what their client requires. If they need to produce a report, in the end, incorporating some costs, then the detail on equipment will need to detail this. TLM recommends open source materials wherever possible, and if used, learners may need to explain the benefits of using these in place of expensive proprietary alternatives. The client may well prefer particular items or brands, or may already have a relationship with a vendor which they would prefer. For example, they may used something like Cisco phones with their routers and switches as they use a complete Cisco Voice Over IP (VOIP) system. If this is the case, then learners will just need to outline what is already in place, particularly if it applies to security.

3.3 I can evaluate the different tools and services available

Learners will make some informed judgements on the equipment and services they have tested

Additional information and guidance

There will be a range of things that learners can do in this instance, but at a very minimum, they will need to say how good or bad some of the equipment and services are. If they recommend a client move to a different ISP, for example, for cost saving reasons of more performance, what are the implications for security. Is the service better, and what services are on offer that they can defend. Some services may offer customers security packages as part of their offering, in which case the learners can identify this and discuss why it is a good feature.

The following is a screenshot from an Internet Service Provider (ISP) showing the features that are available for protecting email services. These are the basic ones, but additional services could be purchased if the client required.

(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');

	BASIC	PLUS	PRO
E-mail Accounts	500	Unlimited	Unlimited
E-mail Storage (per account)	2 GB	2 GB	2 GB
Number of E-mail Aliases	500	Unlimited	Unlimited
1&1 WebMail 2.0	✓	✓	✓
E-mail Forwarding	✓	✓	✓
Anti-spam and Anti-phishing	✓	✓	✓
Catch-all E-mail Addresses	✓	✓	✓
Auto-responders	✓	✓	✓

You can see above that the email has anti-spam and anti-phishing features as well as catch-all addresses so that the client can setup an email such as webmaster@, postmaster@ to go to their client's own main email. Most websites need to have these email addresses for security. There would also be an abuse@ email for people to report problems coming from the client's site.

If the learners use tools like firewalls, how effective are they and can they give examples of what they do?

3.4 I can evaluate the effectiveness of available tools

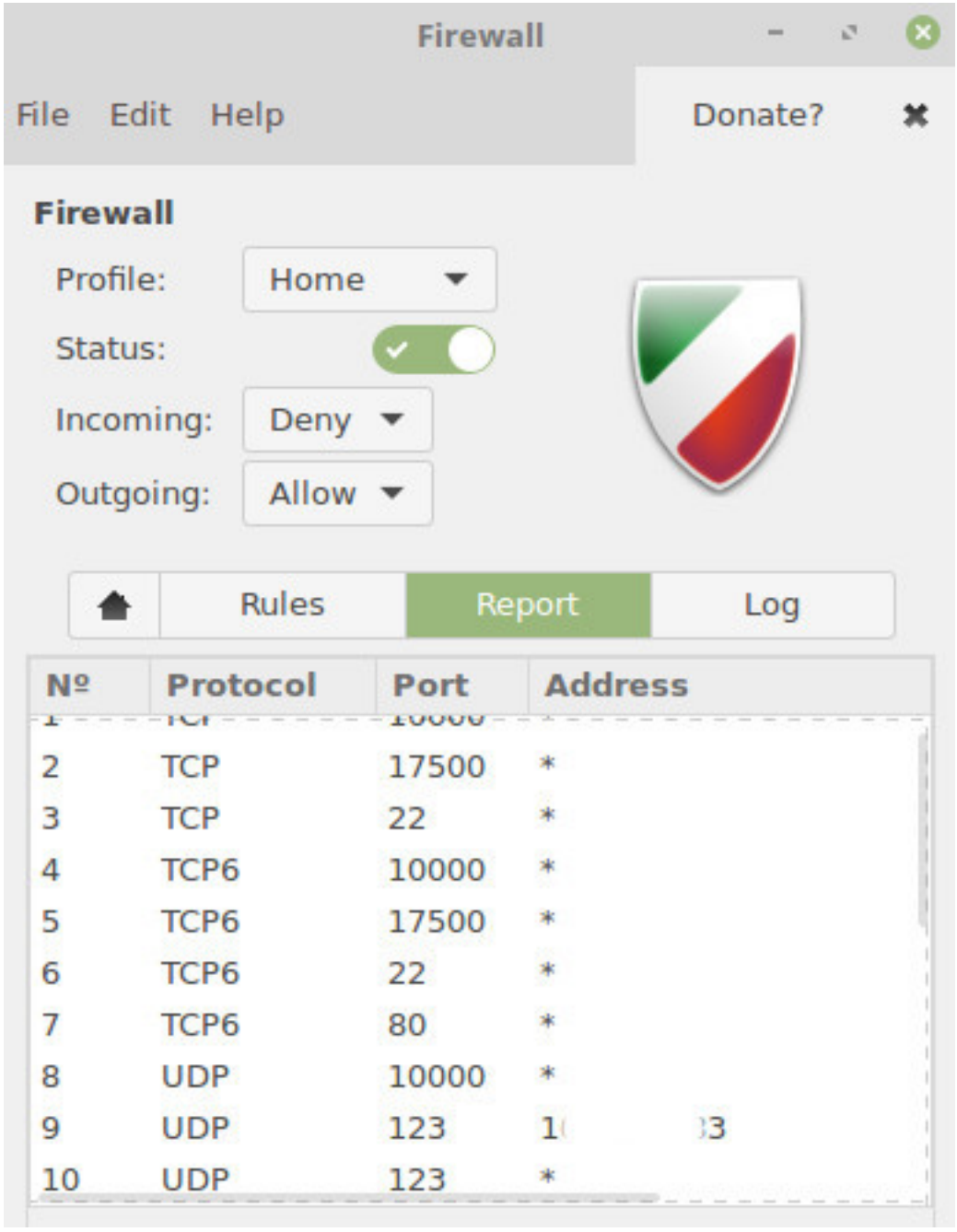
Learners will discuss some strengths and weaknesses of the recommended tools

Additional information and guidance

Most of the detail for the effectiveness will come from logs, assuming learners are able to access these. Some of it might be from literature as they may not be able to get the information required, but should try where possible. Most log files on a home router will show what attacks are happening and what is being blocked. They should be able to show if their own email client whether or not email is being marked as spam. Fishing or phishing emails will be flagged as spam most of the time, but not always. There is no such thing as a perfect system, but they can at least say how effective they think the tools and systems are as this will back up their decision to use different tools. If they can show, even simplistically, that a recommended system has blocked some spam, they could argue that this will enable the client to be more productive. People in offices may spend a great deal of time looking at email to see if it is spam in order to delete it and this will waste their time.

Other tools might be looking at how well a firewall is stopping people from getting in to a network. Most people will know that as soon as your broadband connection goes live it gets bombarded by computes trying to hack into it or look for weaknesses. How effective is their router firewall, or the one the recommended for a client?

The following image shows a firewall desktop software configuration pop-up. The tab that is shown is to monitor what traffic is coming and going to the device it is on.



The one port that seems to be working is UDP (Universal Data Package) on 123. A quick search on something like DuckDuckGo shows that this is the port used by NTP (Network Time Protocol). Computers are very time dependent, down to thousands of seconds, so it is important to be accurate. In this case, the computer has been set up to get the correct time across the Internet via atomic clocks based in London. The computer is sending UDP packages though port 123 in order to update the computer's time every few seconds. The client computer should allow NTP packages through port 123, but should block any other packages on that port.

In the image above, you can see that the firewall is checking TCP and UDP traffic, which is IP v4 traffic, but also UDP6 and TCP6 which is IP v6 traffic. Learners can investigate these, but is not essential.

The documentation for the firewall shown above gives some useful examples.

https://help.ubuntu.com/community/Gufw [4]

3.5 I can evaluate the effectiveness of a system overall

Learners will make some informed judgements about their work overall

Additional information and guidance

How good were the tools they recommended and hopefully setup at blocking unwanted access or traffic? Do they have any data to backup their findings? This data can be qualitative or quantitative.

Qualitative - my client commented that they got far less spam email and could therefore work without distraction.

Quantitative - my recommended system was able to reduce spam by 40%.

Some examples, especially from the client, would be very helpful here. It might be useful for learners to create a feedback from or questionnaire to give to their clients to gather some feedback comments that they can use. If it is easier, they can create a survey using an online system such as Survey Monkey as it will automatically create charts and summaries of the data for them.

https://www.surveymonkey.com/ [5]

It is not always easy finding “faults” in something they have worked on, but learners should be encouraged to think about possible improvements. Perhaps the user guide they created was too wordy and needed more pictures to make it clearer. Perhaps the pictures are not clear enough.

3.6 I can describe the laws that regulate online safety

Learners will describe the main laws that govern the safety and security of online users

Additional information and guidance

There are various laws that learners could investigate in relation to online security and protection. The most familiar ones will be:

- The Data Protection Act 1998
- The General Data Protection Act 2016, General Data Protection Regulation 2018
- Computer Misuse Act 1990
- Copyright laws
- FAST (Federation Against Software Theft) 1984

Learners can research these and others and recommend how they protect people from online issues. They will need to do some research as the criterion asks them to **describe** the laws. Some useful examples would help it to be more clear to people looking at the work.

What laws affect the learners that they are aware of? Do they know the punishment for copyright abuse or piracy etc. How well do the laws protect people in the globalised world of online access?

Source URL: https://theingots.org/community/sil2u81x

Links
[1] http://www.clamav.net/downloads
[2] https://answers.microsoft.com/en-us/windows/forum/windows_10-security/wanna-cry-ransomware/5afdb045-8f36-4f55-a992-53398d21ed07?auth=1
[3] https://eportfolio.tlm.org.uk
[4] https://help.ubuntu.com/community/Gufw
[5] https://www.surveymonkey.com/