

Unit 2 - The Analysis and Understanding of Cyber Threats

Overview

The candidate will display an understanding of cyber threats through some analysis of potential attacks and how systems are designed to deal with them. They will explore the workings of a system through the model of the OSI as a framework to look at both hardware and software and associated services. They will then explore and document the aspects of the system that are attacked, such as the ports used as doorways or the vulnerabilities that are part of a working system. They will evaluate these processes and be in a position to make some basic recommendations for improvements.

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 – a report to the school governors of a local primary school to show the extent of threats.

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 this 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

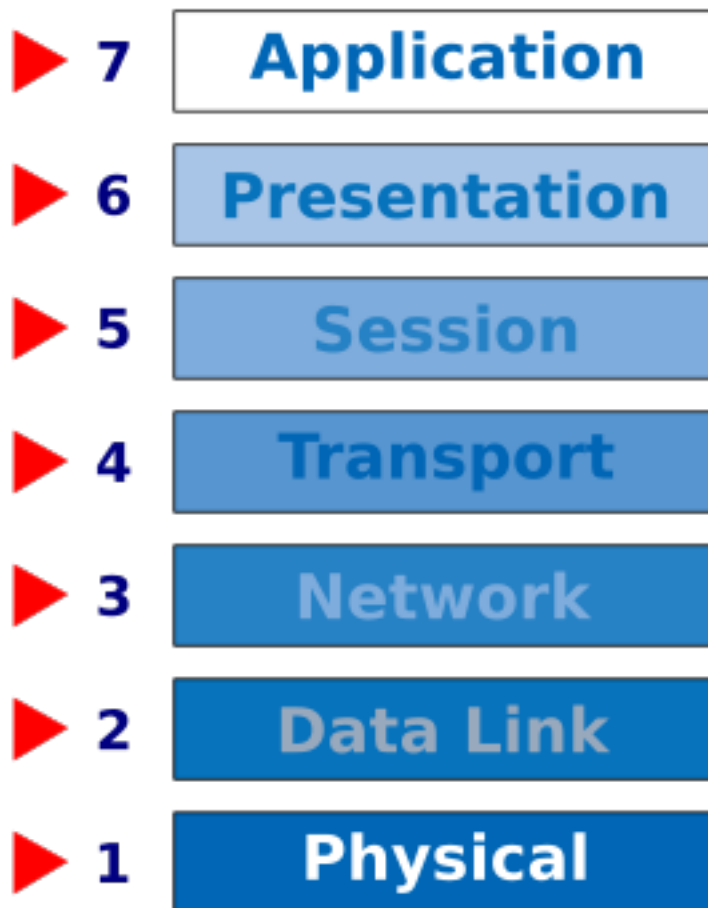
1. Understand the parts of a system that are attacked

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, udp etc.

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 security. What aspects of hardware may be compromised by people trying to break 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

Unit 2 - The Analysis and Understanding of Cyber Threats

-->

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 with 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.

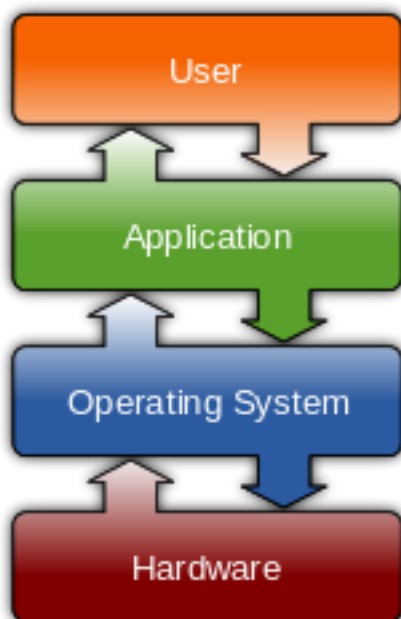
1.3 I can explain the main software features of an IT system

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

Unit 2 - The Analysis and Understanding of Cyber Threats

-->

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.

Subject: You have notifications pending
From: " Facebook 2 friend request" <support+17wgm3rptvn3@lpl.com>
Date: 03/05/17 02:45
To:

facebook

Hi,

Here's some activity you have missed on Facebook.

[2 friend request](#)

[Go To Facebook](#) [See All Notifications](#)

This message was sent to [Facebook, Inc. Attention: Department 415 P.O Box 10005 Palo Alto CA 94](#) [If you don't want to receive](#)

▶ 1 attachment: You have notifications pending .eml 5.9 kB

http://toolcenter.nl/aspnet_client/leyland.php

The mouse held over the blue hyperlink reveals the actual link, in this case http://toolcenter.nl/aspnet_client/leyland.php [1].

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

```
(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');
```

```
leyland.php x
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() { yeta=77; 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.

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	Comment
25	smtp (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

```
(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');
```

Unit 2 - The Analysis and Understanding of Cyber Threats

-->

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.

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> [2]

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

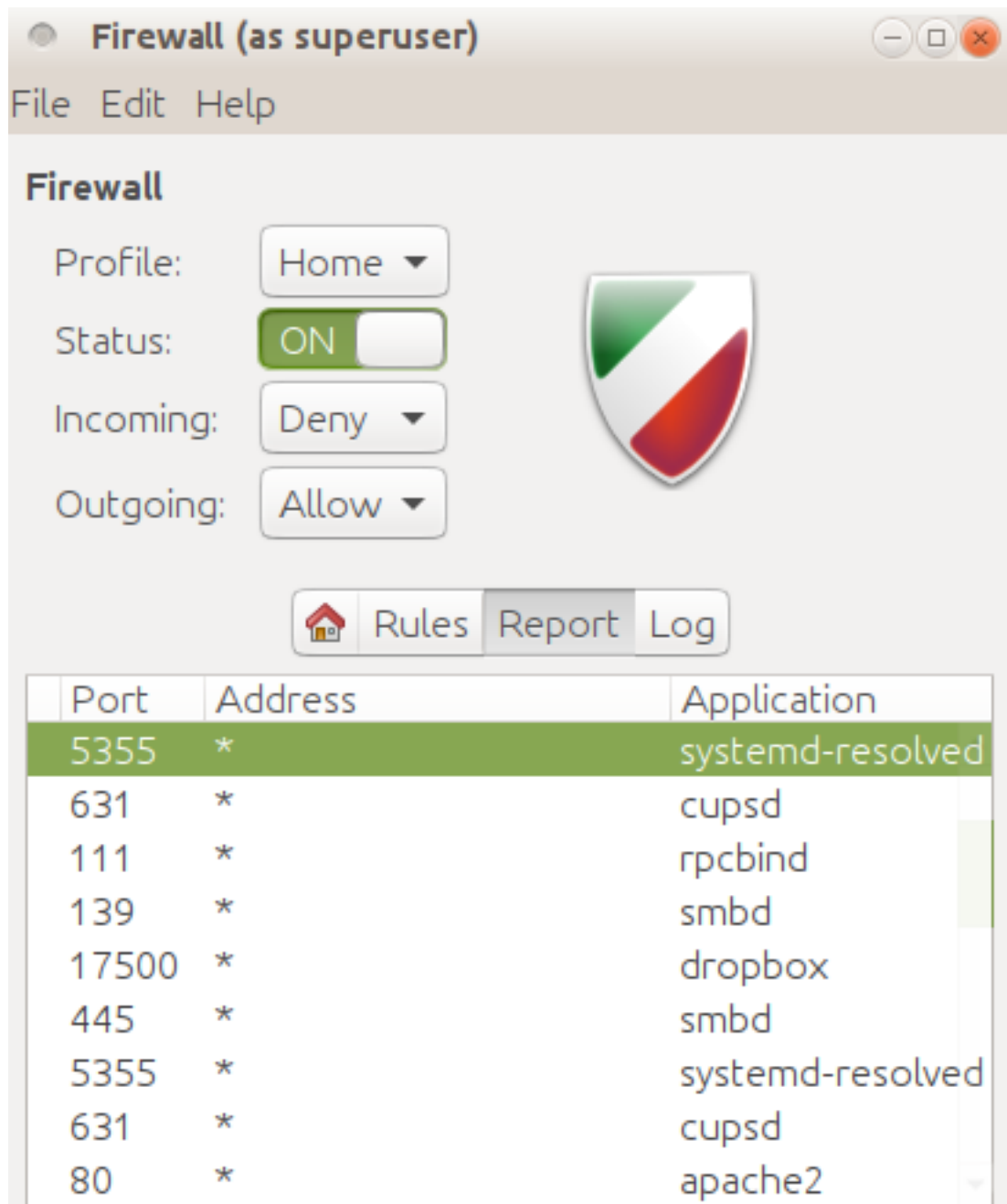
Additional information and guidance

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.

Unit 2 - The Analysis and Understanding of Cyber Threats

-->

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

Unit 2 - The Analysis and Understanding of Cyber Threats

-->

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 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 (the 2017 Wannacry attack on various countries was based on the Windows SMB Protocol). 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 has some flow control to check if they arrived, but UDP one doesn't. The web server will accept request 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 of 8080.

Learners don't need to go into detail here, just to show that they understand some association between these. As there are 65536 ports on a computers (this includes port 0 which is often forgotten) it would be impractical 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 port are effectively door 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, and most of these are pirated so will not be updated. These are ideal to

```
(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');
```

Unit 2 - The Analysis and Understanding of Cyber Threats

-->

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 and easily 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 and free Linux operating systems and the huge market potential means that millions of routers were created and sold and all had 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> [3]

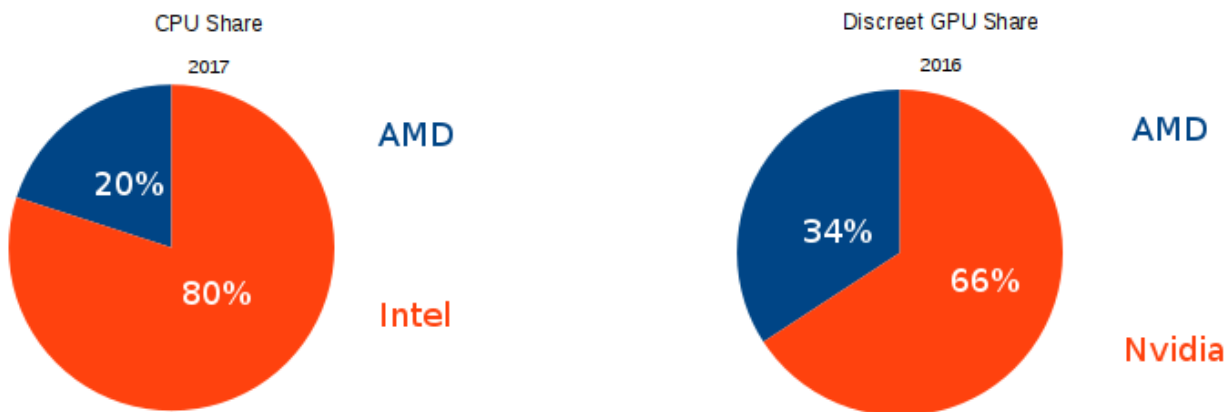
Learners can research various articles on the Internet and report on some of the ways different parts of the system are attacked. The doll attack is clearly the top application layer. What about the session level with https spoofing and similar.

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 and 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.

Unit 2 - The Analysis and Understanding of Cyber Threats

-->

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 [4]

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.

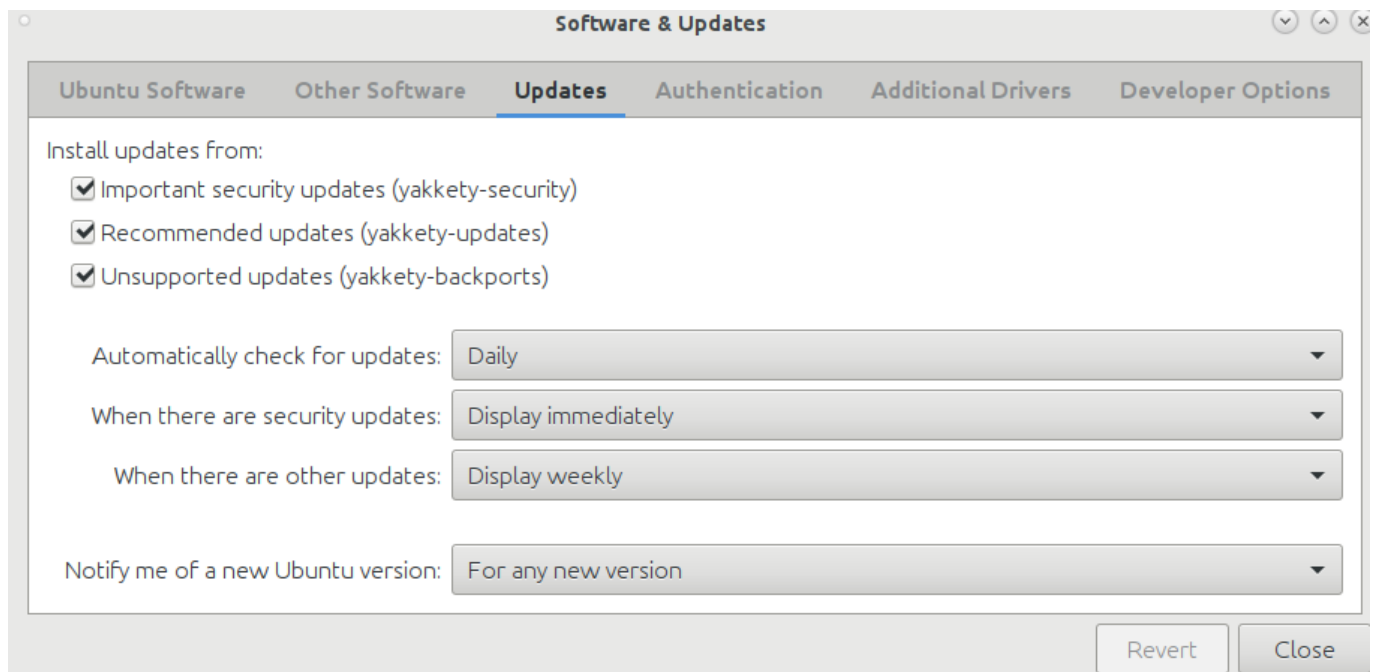
Learners can demonstrate they understand that hardware is not immune from being hacked.

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 admins 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 di

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

```
(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');
```

Unit 2 - The Analysis and Understanding of Cyber Threats

-->

There are extensive way 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 [5]

- Security exploit - SQL injection, XS scripts, exploits of ftp, http etc.
- Brute force attack
- 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 [6]

This may for a 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 can be attacked and made 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 and necessary links or further information a client may require

Source URL: <https://theingots.org/community/sil2u71x>

Links

- [1] http://toolcenter.nl/aspnet_client/leyland.php
- [2] <https://www.co-operativebank.co.uk/global/security/card-reader>
- [3] <http://www.bbc.co.uk/news/world-europe-39002142>
- [4] https://www.cl.cam.ac.uk/~sps32/mcu_lock.html
- [5] https://en.wikipedia.org/wiki/Security_hacker#Attacks
- [6] https://www.owasp.org/index.php/Top_10_2017-Top_10