Network protection

1. Network security - prevention methods

The types of threats to network security have been discussed in another section.

There are many different things that can affect security on both a network and a personal computer. Over the next few pages we take a look at some of the ways to help reduce the risk of being affected by these threats.

Network protection

2. User access rights

On a network not everyone needs access to every single file except the system administrator.

At school, you can expect to access your own files but not other peoples' unless they are in a shared area. Students cannot see staff areas - nor would they expect to. Beyond that teachers cannot see school office areas.

For this to happen, 'user access rights' are applied to the files and folders on the network.

User access rights is set up by the network manager who defines groups and allocate specific permissions to those groups. People using the network will then be assigned to a group and all permissions related to that group will apply to them when they log in.

For example, a group called 'students' might be able to view the student shared area but not make any changes to files in that folder. Whereas a group called 'teachers' can view the shared area and also add and delete files.

The three common access rights are

- 'Read', which is the ability to view and open the file or folder.
- 'Write', which allows the file or folder to be modified.
- 'Execute' which gives the user the right to execute or run an executable application.

These rights can have further restrictions placed on them. For example:

- Access can be restricted to particular workstations or terminals
- Access can be restricted to certain times of day
- Accessing can be flagged so that others are notified when someone opens or changes a file

Having this level of control over user access rights helps maintain network security and ensures that people only have access to areas they have the authority to use. And if there is virus or malware, it is limited to the areas that this user has access to.

Network protection

3. Passwords

A password, along with a user name is the most common way of protecting a network. To get access to the network, a user has to correctly enter both their user name and the password associated with it.

However, the *quality* of a password matters a great deal.

The most basic way to guess a password is called the 'brute force' approach. This means a computer program is written to go through every possible combination of letters (and / or symbols) until the right one comes up.

For example, there are 26 letters in the English alphabet, so it would only take 26 guesses to find a 1 letter lower case password (obviously useless as a password!).

So to make a strong password, you want to increase the number of guesses a computer would have to make, by either making the password longer or by including non-alphabetic characters.

Simple password quality

Password	**Length**	**Maximum combinations of letters**	**Online attack 1000/sec**
abcd	4	1/2 million	< 10 minutes
abcde	5	10 million	< 4 hours
abcdef	6	300 million	< 4 days
abcdefg	7	10 billion	up to 3 months
abcdefgh	8	Lots	up to 7 years

The problem with long, random passwords it that people just cannot remember them.

One solution to this is to use a **password manager**.

This is a software application designed to handle your passwords by automatically creating long, random passwords for your favorite sites and password protected files. Then it inserts that password automatically when it encounters the site or file.

Network protection

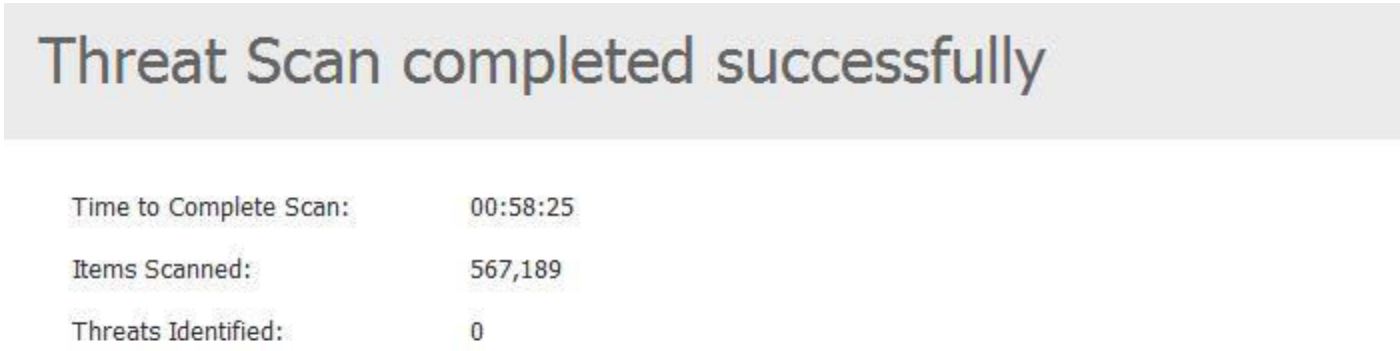
4. Anti-malware

One of the biggest threats to network security is malware. As such, companies have produced software specifically to protect networks against viruses and malware.

Anti-Virus

This application is designed to detect computer viruses. It has a database of virus 'signatures', and also looks out for typical virus behaviour such as modifying important system files. The virus database is downloaded and updated on a daily basis, as new or modified viruses are constantly discovered by the anti-virus company

This is what you want to see when an anti-virus or anti-malware scan is carried out.



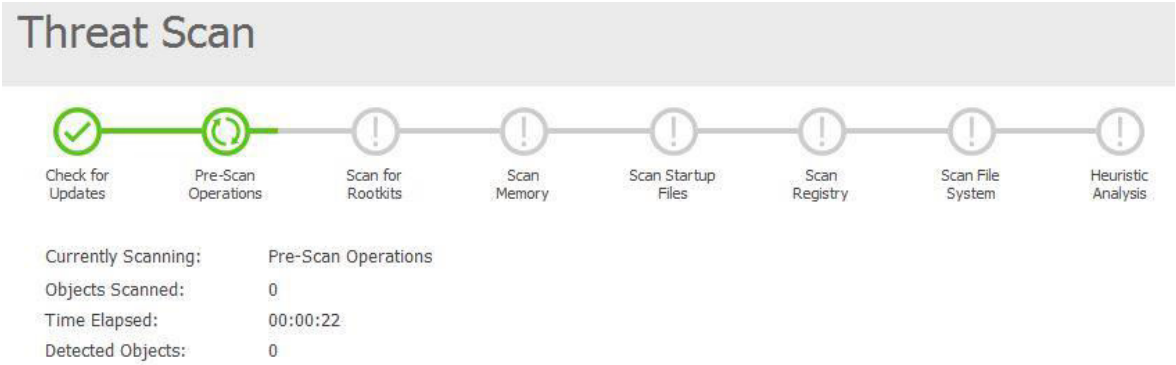
If a problem *is* detected, then that file can be 'quarantined' or an attempt made to repair it.

Anti-malware

Not all malware are viruses. It could be a program designed to detect key strokes, which is a form of spy-ware. Or malware that quietly allows remote

control of the computer, and so on. these types of malware can also be detected and removed by anti-malware software.

The screen below shows the computer areas a good anti-malware program examines. The hard disk is scanned first (root kits), then RAM memory, followed by individual files and registry entries. The system itself is then scanned and finally 'heuristics' which looks for known malware behaviour rather than a specific threat.

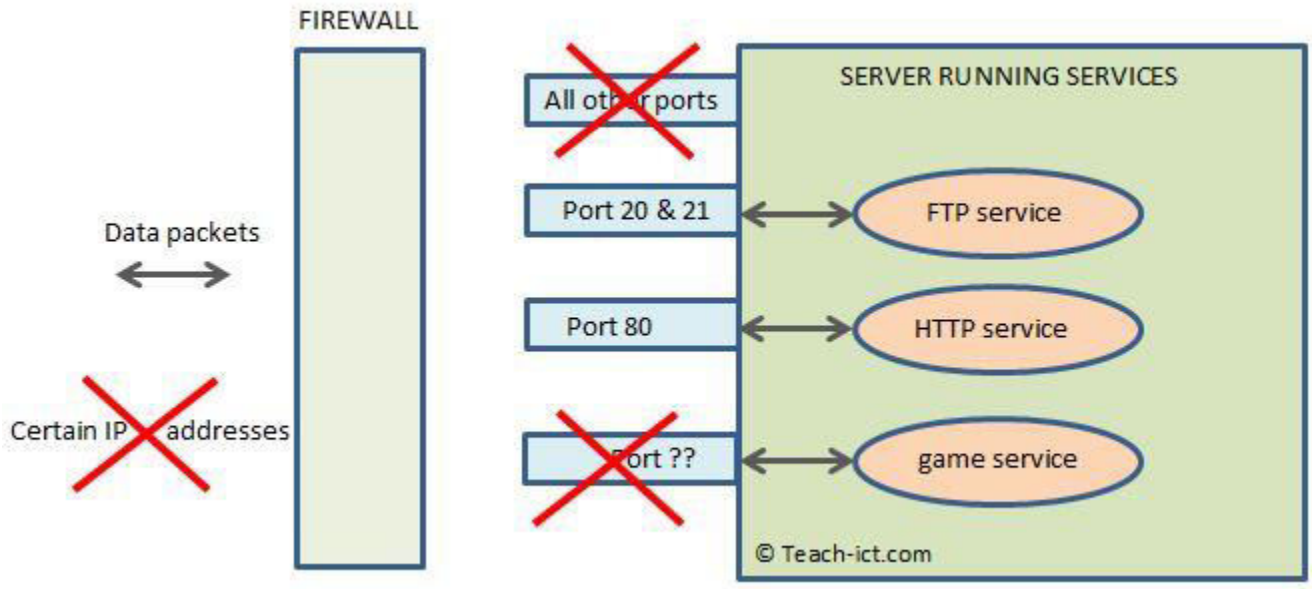


Network protection

5. Firewall

A 'firewall' sets the rules for how data packets can enter or leave the network. Firewalls can be a hardware appliance or software running on the local computer.

The diagram below shows a firewall in place that is blocking certain access points (ports) and network addresses.



As you can see, the port that the game service used is now blocked. This is why a firewall often causes a problem with online games, a rule needs to be added to allow the ports they want to use to be open.

The firewall also has rules in place to block access to certain IP addresses. For example, many schools use their firewalls to block student access to YouTube and Facebook.

Firewalls help protect against Denial of Service attacks, and can prevent malware from leaking data back out of the network if it manages to get in.

Network protection

6. Penetration testing

An excellent way of finding weaknesses in a network is to hire professional 'hackers' to actually try and get into the network..

It is unkind to call them hackers as they are fully professional experts in testing the weaknesses of a network - perhaps we should call them 'penetrators'.

They use the very latest penetration tools, and maybe some they have designed themselves.

To make the job realistic, they are not provided with any extra information about the network itself as that would give them an advantage; just what they can gather from publicly available sources.

Before they begin, they have a legal contract with the company that makes it very clear what they can and cannot do on the network, as normally a hacking attempt is illegal under the UK Computer Misuse Act.

Once they have carried out the task, a report is given to management about any weaknesses found and suggestions as to what they can do about it.

Network protection

7. Encryption

Even if a network or file is accessed by an unauthorized person, another line of defence is to make confidential data unreadable.

Encryption is the process of scrambling a message or data in such a way that only the person (or computer) knowing the correct key can read it. To anyone else, it looks like gibberish.

The **plain text** i.e. unencrypted message might be

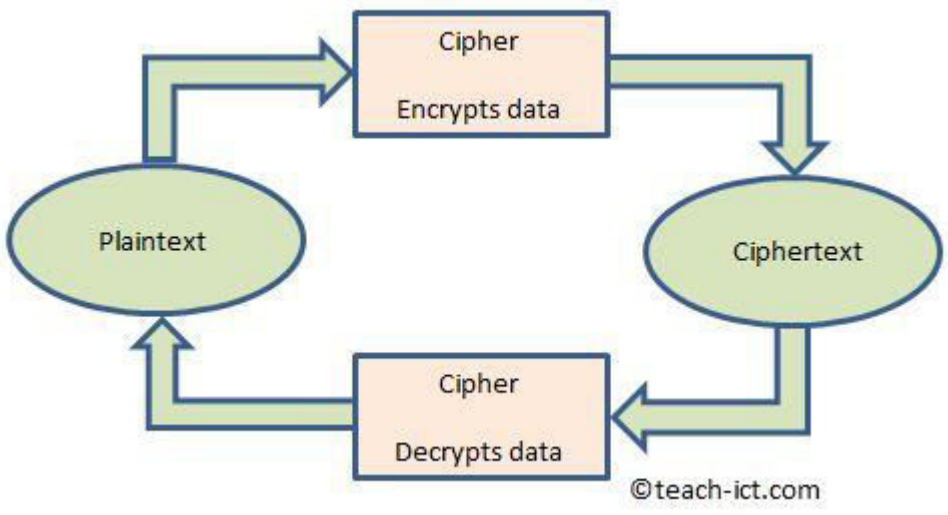
My birthday is 4th April 1966

And the **cipher text** i.e. encrypted text looks something like this:

!£jdii£$88jhassaijaoa8890034nnakak££*&&22992

The method used to encrypt the message is called a '**cipher**'. There are many strong ciphers available such as AES-256.

The diagram below shows the process of encrypting and then decrypting using a cipher.



Encryption is based on mathematics. A '**key**' is a very large random number, usually up to 256 bits. The key is applied to the plaintext through a very

complicated maths procedure called a 'cipher'. For example the industry standard AES-256 cipher uses a 256 bit key.

Network protection

8. Physical security

A good method to avoid direct vulnerability is to simply make it difficult for unauthorised people getting access to the server or computers.

In data centers for example, where security is paramount, you can expect all the typical physical security systems to be in place, these include

- External fencing and alarms
- Biometric or security cards to open doors
- Secure cages around individual sensitive servers, each cage allowed by specific people.
- CCTV cameras and security staff.
- USB server ports disabled, physical and operating system (preventing Hollywood style 0-100% download excitement 'will-I-do-it-in-time' possible)
- Server keyboards locked away in steel boxes
- Tethered computers with steel cable
- Alarm systems to detect physical tampering such as taking a cover off
- 'Air-gapped' servers that have no physical or wireless connection to the Internet
- Thick walls that are hard to break through, no windows
- External maintenance people accompanied at all times
- Floor-to-ceiling single person turnstiles to prevent piggybacking
- A two door 'airlock-style' entry for equipment and for persons with disabilities

- The most secure is an air gapped "Tempest" faraday cage where not even the electronic emissions of keyboards or monitors can be picked up remotely.

This is over-the-top for most establishments but even the most casual offices could include some of these measures to protect their computers and physical access to the server.

Network protection

9. Summary

- *User Access Rights* limits what each network user can access.
- *Passwords* need to be strong to maintain security.
- *Physical security is used to prevent direct access to computers and servers*
- *Anti-malware and Anti-virus* applications are installed to detect issues.
- *A firewall* controls the data packets that can flow in and out of the network.
- *Penetration testing* is a way of trying to find network weaknesses.
- *Encryption* make confidential data unreadable unless the decryption key is used.