IT Security Threats & Cryptography

LUKE PERRY (P110104969)

Luke Perry

Contents

Physical Security

An effective way to secure a system is to make a user use something they are, have or know in order to able to gain access to the system. When two-factor authentication is used it will require two pieces of information however it can't be taken from the same category. For example, a user needs to a PIN code and a card to use an ATM and this is something they have and know.

Things That You Are

Biometrics

Types of biometric security include facial recognition, fingerprints and retina scans. This is a very secure type of security as it can be a hard thing to replicate as biometrics are unique to every person. Therefore, it can be difficult for an attacker to bypass this type of security without advanced pieces of technology.

Voice Control

While voice control is a good type of security as it will only activate when a specific phrase is said by one person it has its downfalls. This is because if someone is able to record the person saying the phrase then they could clear the audio up to make it as clear as possible then use that to get through the voice control.

Things That You Have

Card Key Entry

Card key entry is when a door requires a specific card and sometimes also a PIN in order for the door to open. This type of security while effective can also be a bad way to protect your organisation as it can be very easy for someone to lose their card. If this happens then anyone who finds the card will be able to access the room unless there is also a PIN code as then they will have to figure that out as well which makes this type of security a lot more secure.

Closed Circuit Television (CCTV)

CCTV is a very effective piece of security if a breach of security has happened as it will allow people to review footage of what has happened. Therefore, if someone was to steal something then the footage could be reviewed and analysed in order to find the person that stole the items.

Things That You Know

Passwords

In order to create an effective password, it should include a mix of capital and lowercase characters, numbers and special characters. However, a lot of people are lazy with their passwords and just create simple and easy to remember passwords therefore two factor authentications can be really effective when using this security technique. With a google account for example it will require your phone to give you permission when you sign in on a computer in order to actually log in. This is a good type of security as even if someone knows your password they will still need your phone in order to actually sign in to your account.

Software Security

Anti-Virus Software

Anti-virus software is installed in order to try and pick up on malicious files and remove them. With Windows 10 there is a built-in anti-virus which is Windows Defender. If a file that could be classed as dangerous of malicious is found then Windows Defender will warn you to see if you want to keep it or remove it. However, in some cases if the file is seen to be really malicious then the file will just be

deleted straight away without asking if you want to keep the file. This security is very good for computers as it is one of the best ways to protect yourself from viruses, worms, trojans and any other types of programs that an attacker may try to use.

Firewalls

A firewall is similar to anti-virus software with the difference being that firewalls are connected to computer networks. If there is any suspicious data going in or out of a computer to a network the firewall will pick up on it. This will stop computers from becoming bot or zombie computers and also stop them from spreading worms and viruses. Therefore, firewalls are extremely effective when there is a computer connected to the network and when paired with anti-virus software there computer will be very well protected.

User Authentication

User authentication is an effective piece of security as it requires a piece of information only one person knows. However, this can also not be effective as if the authentication is only a password then there is a load of people that just use easy to remember and short passwords. This makes some accounts easy to brute force. On the other hand, if someone has a strong password and also uses two factor authentication the account becomes very secure as it doesn't only require something the user knows but also a piece of information the user either is or has.

Plan

Risks

- Unsafe software could be installed from the Internet
- Non-admin users might be able to use control panel in order to change important settings
- Some files might contain malicious data and if the system isn't checked frequently these may not be picked up
- Natural disasters could strike
- Hardware could become corrupt or get stolen
- Untrained staff might be using the system incorrectly

Contingency Plan

- Have data backed up at offsite locations as well as onsite in case any versions become inaccessible
- Use a virtual machine to test any new security settings to make sure they work first before being implemented into the actual system

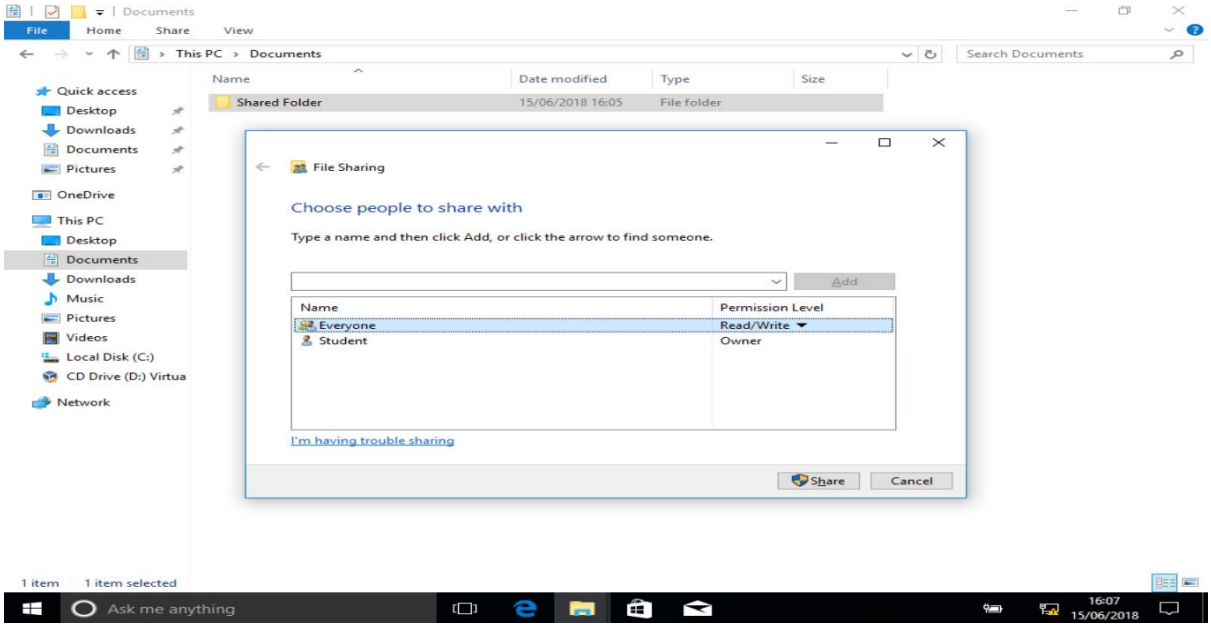
Actions

- A shared folder will be setup so users will be access each other's files
- A firewall will be setup to protect the system and restrict access to it
- The firewall will have an activity log so it's easy to track what happens on a system
- Anti-virus software will be configured and a scheduled scan will be setup
- Control panel will be disabled for non-admin users

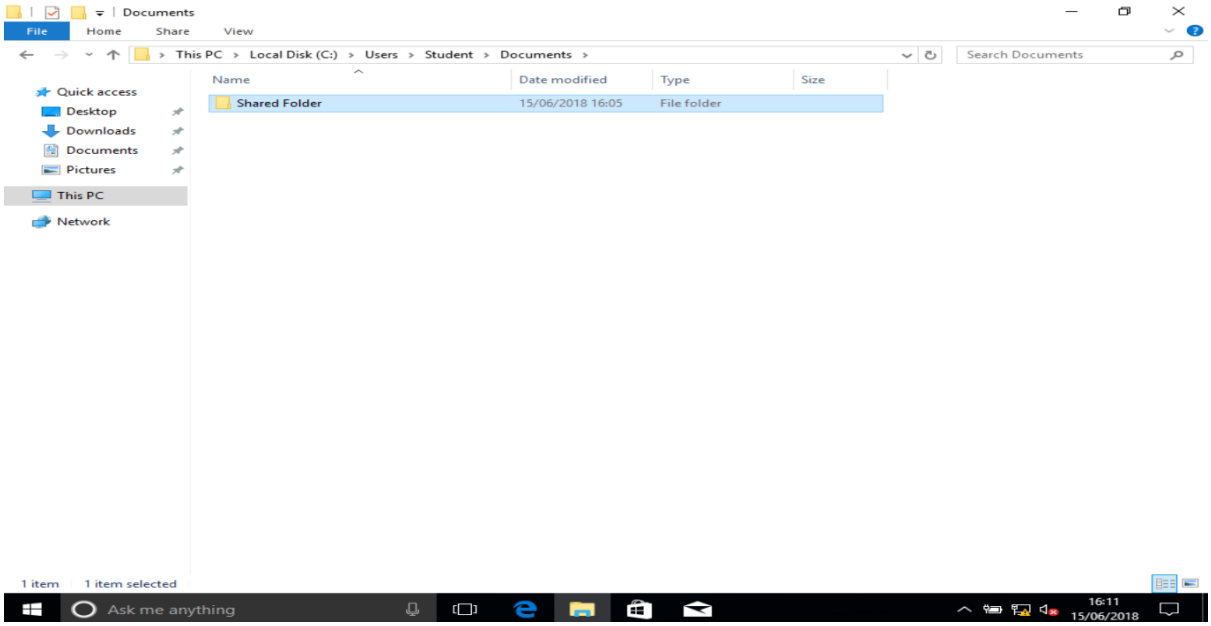
Test Plan

- Test the shared folder on multiple accounts to make sure everyone is able to access it
- Check non-admin accounts to make sure they can't access the control panel
- Run a scan using Windows Defender to make sure that the anti-virus is working
- Run a program that requires permission to run to make sure it's logged in the firewall event log

Shared Folder



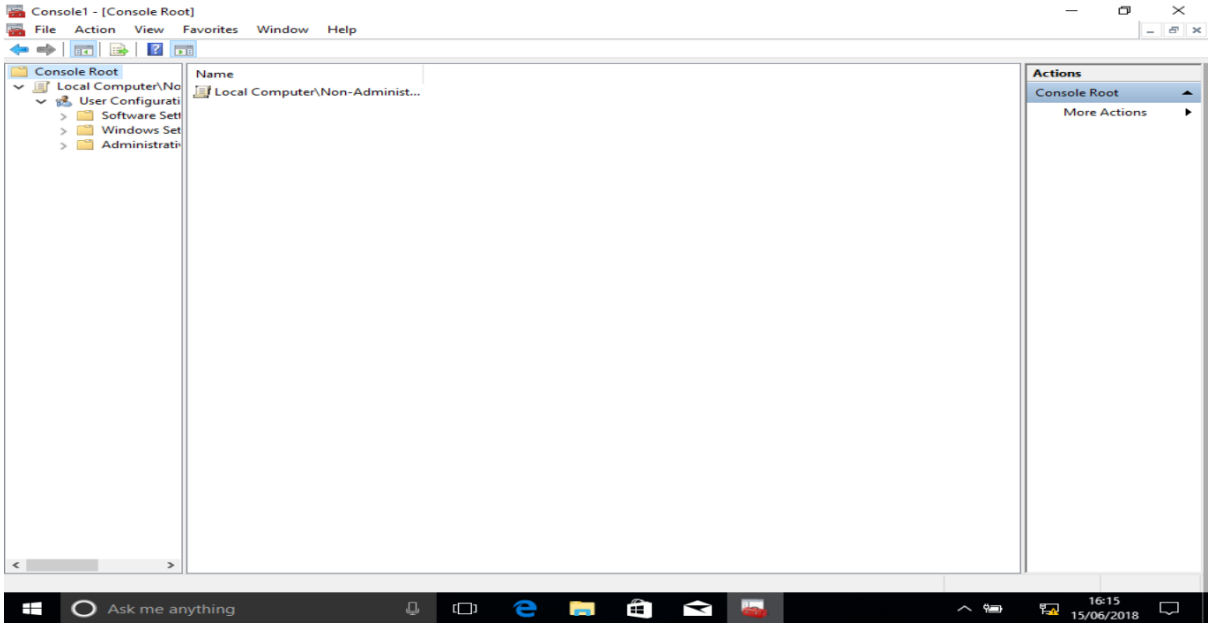
In the above screenshot I'm setting up the shared folder on the admin account and setting it so everyone is able to read and write to the folder.



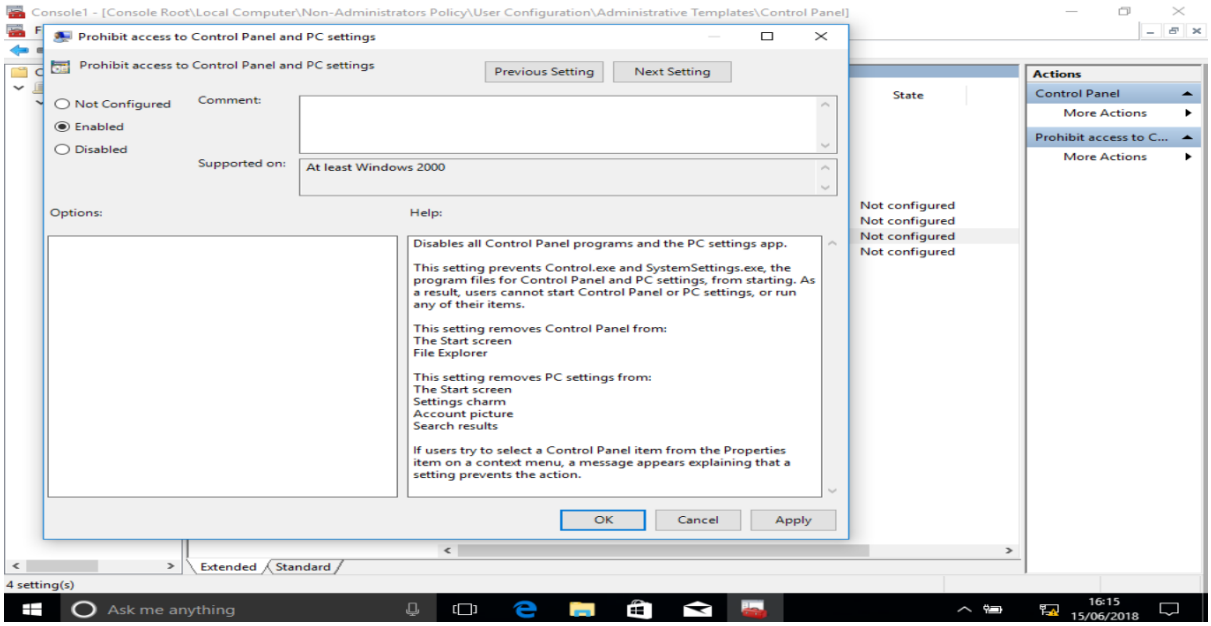
In this screenshot it's showing the folder being accessed on the non-admin account.

Shared folders will be useful for when some people in the business will need access to certain files so folders can be made available to everyone, specific employees or just admin staff. This makes sure that random people can't changes certain data in the files making the security of the software being produced better as it can reduce the risk of internal attacks from employees.

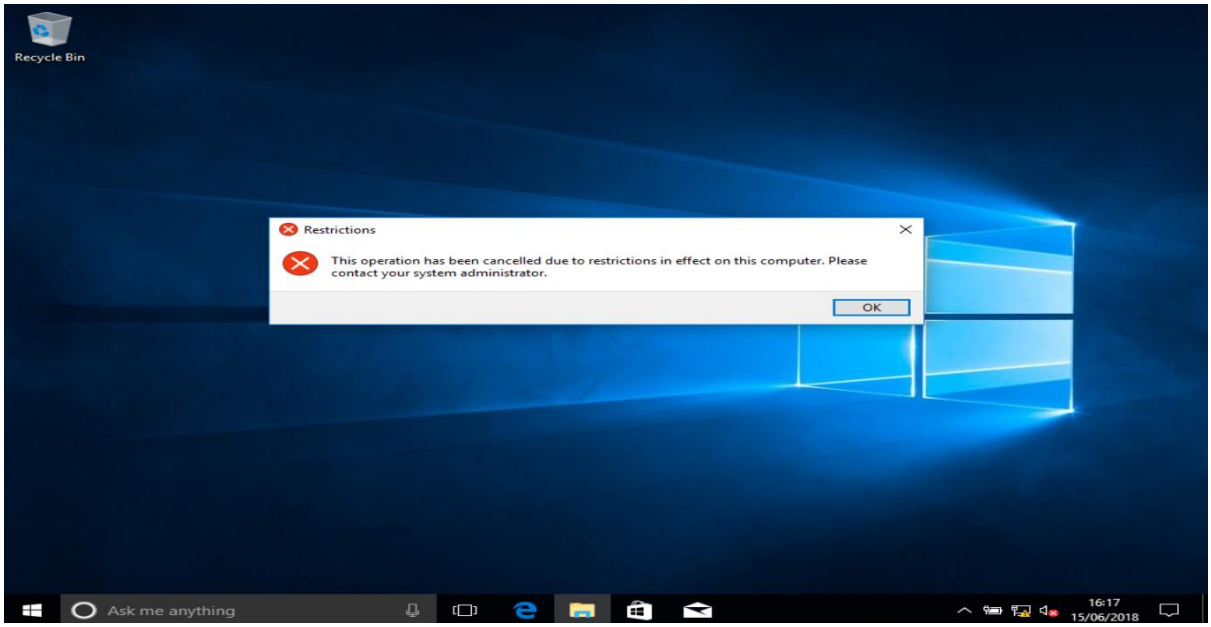
Group Policies



The above screenshot shows me going into the group policies so I'm able to setup conditions for non-admin accounts.



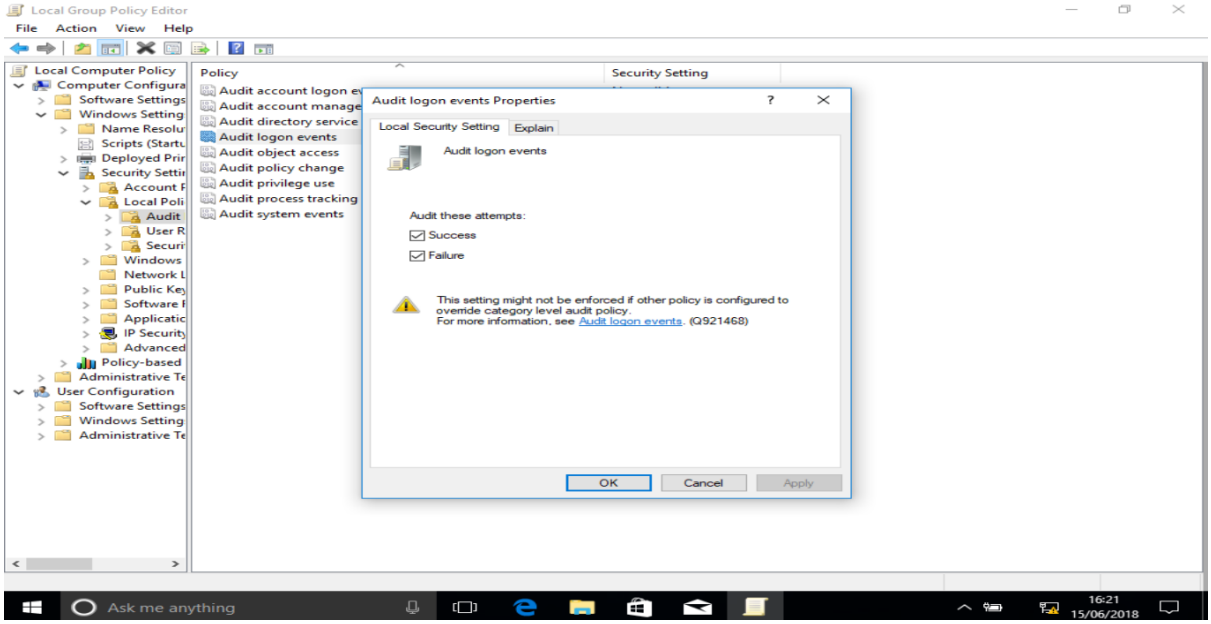
This shows me enabling the option to disable control panel on all non-admin accounts so it won't be able to be accessed by most users.



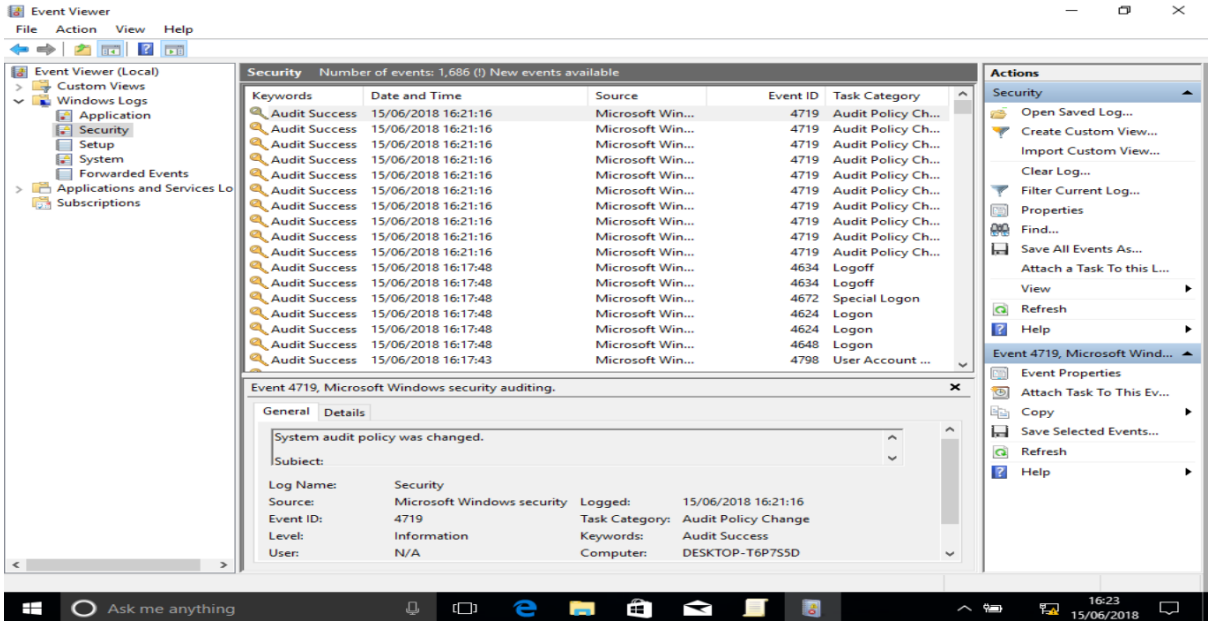
This screenshot shows the error message when I try to open the control panel from the non-admin account.

I set this up on the system as it stops anyone without proper authority from making significant changes to the system which should prevent the amount of errors that can occur.

Audit Policy



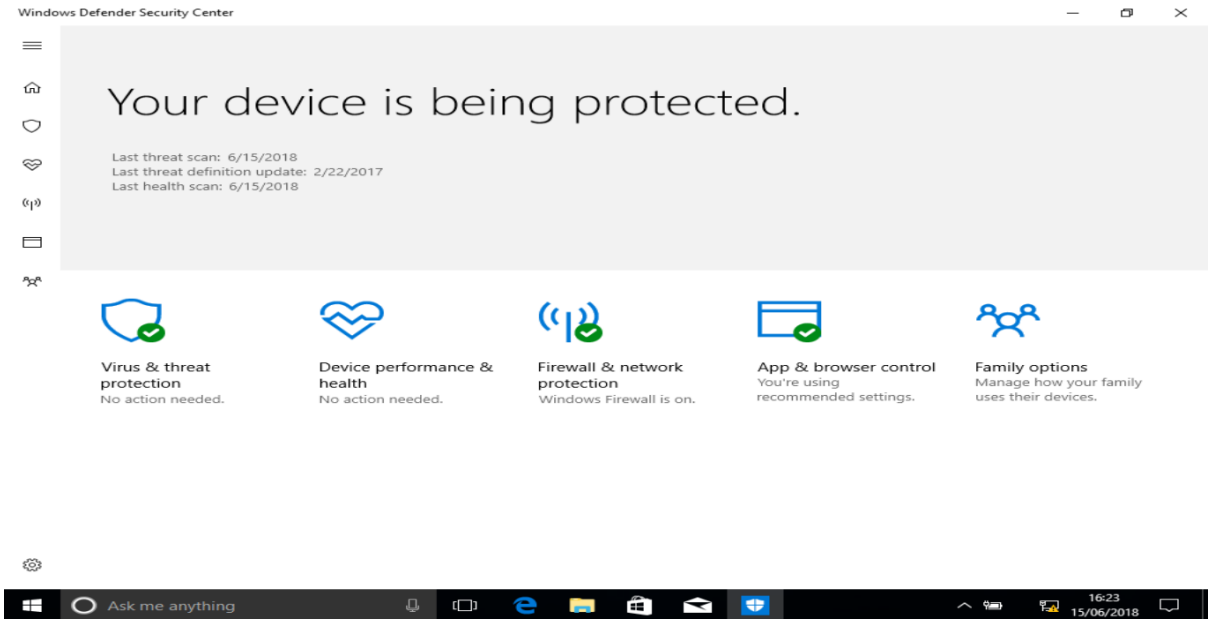
The first screenshot shows me setting up the auditing log so it logs all successful and failed attempts.



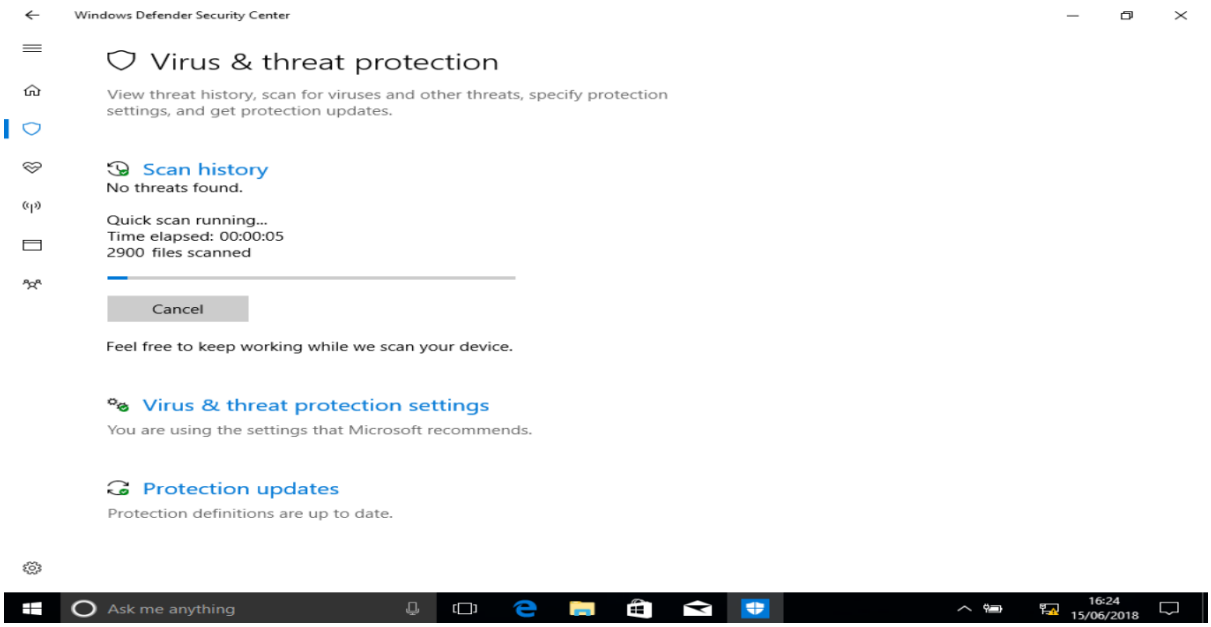
This shows me accessing the audit log.

I have set up an auditing log so whenever someone accesses particular files it will be recorded in the log showing who it was that tried opening the specific file along with whether they were successful or not. This is effective for security on the system so it can be checked and if any suspicious activity can be spotted then it should be able to reduce the amount of inside attacks that could happen.

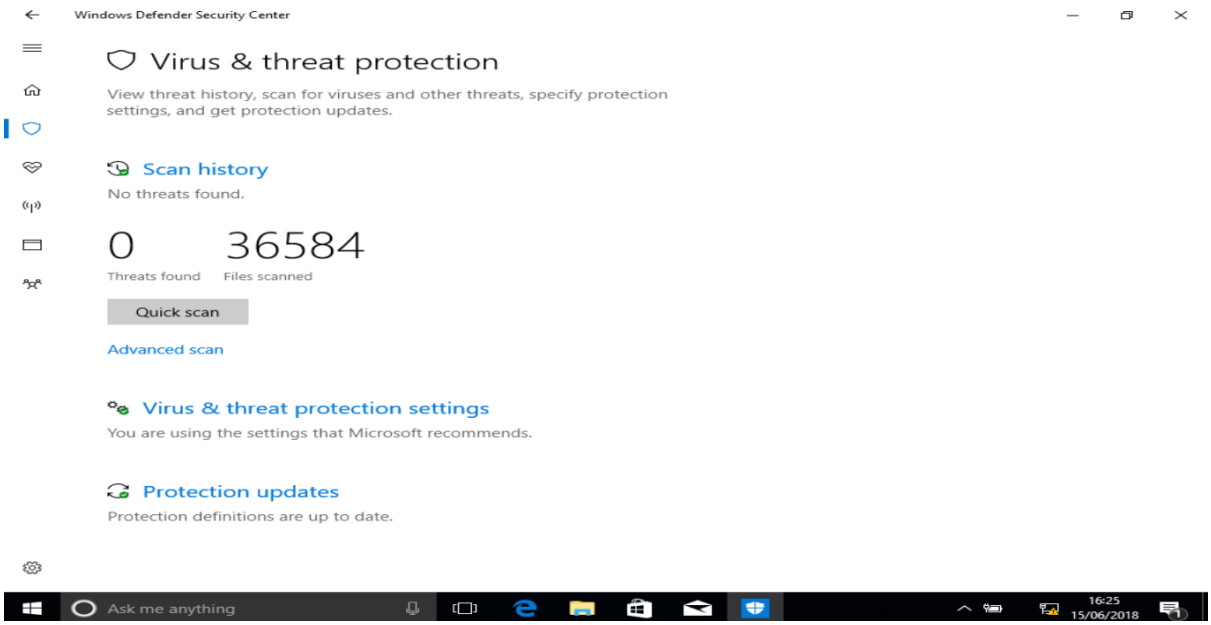
Windows Defender



The anti-virus software being set up can be seen above.



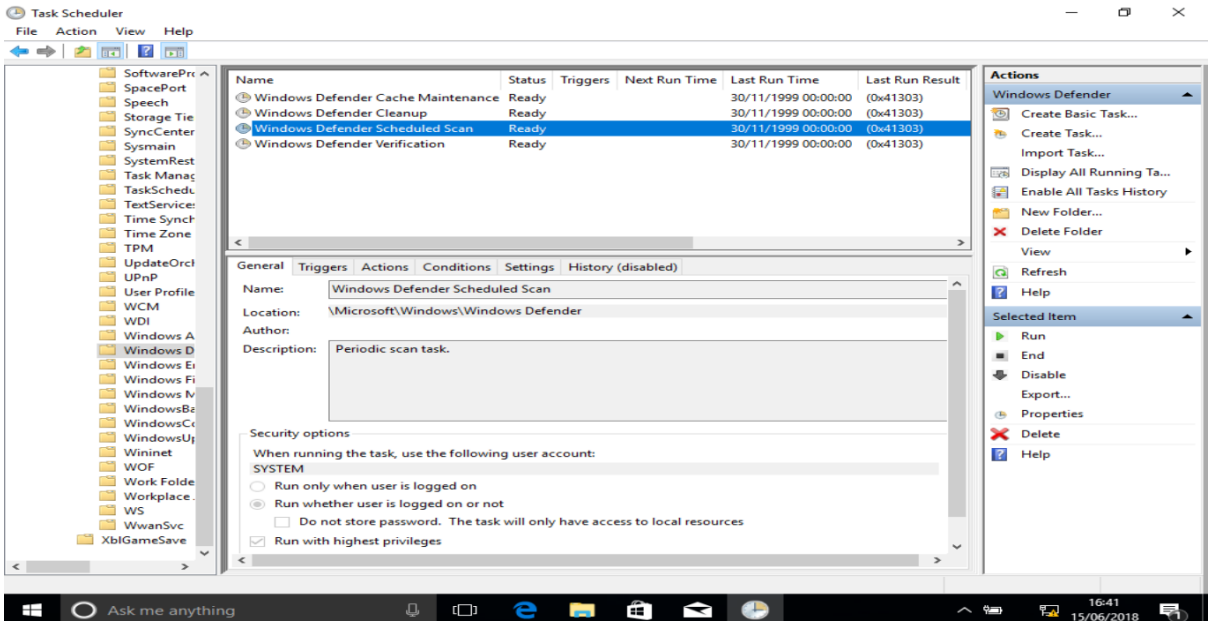
This screenshot shows that I have started a scan and the system is getting its files checked.



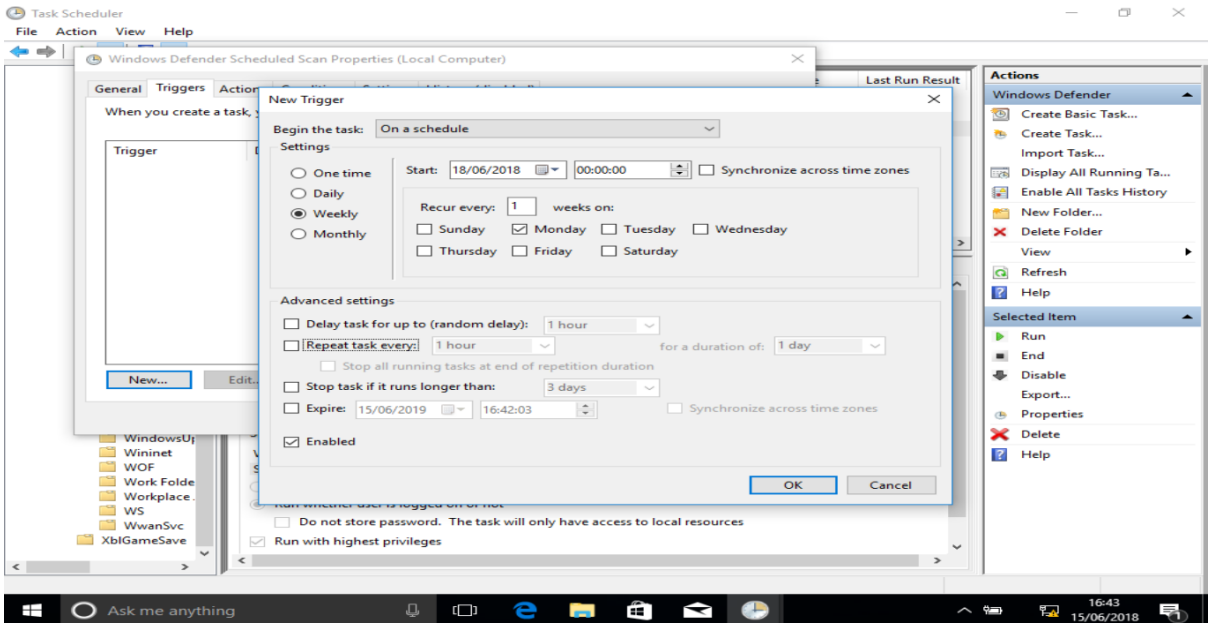
As seen above, the system has been completely scanned and no threats have been found.

I have setup Windows Defender on the system so anti-virus software is installed in order to try and find any files that may contain viruses, worms or any other harmful pieces of software. As seen in the screenshots I have setup the anti-virus software and performed a scan to make sure that all the files currently on the system are safe.

Scheduled Scan



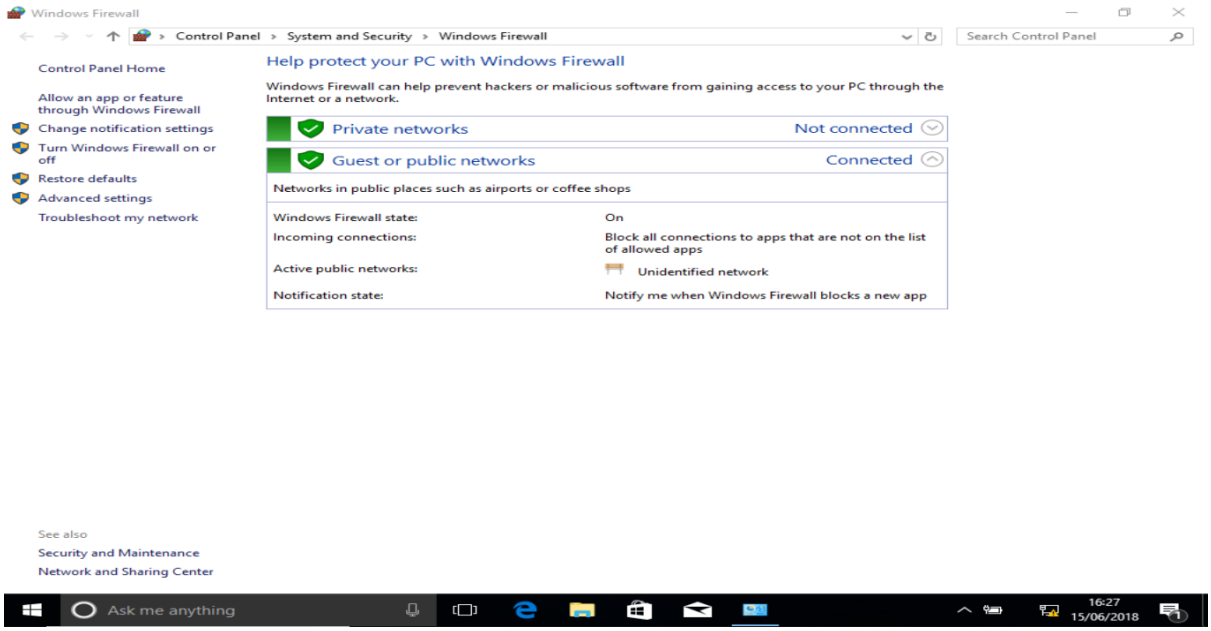
This shows that I have gone into the settings for Windows Defender settings in order to set up a scheduled scan.



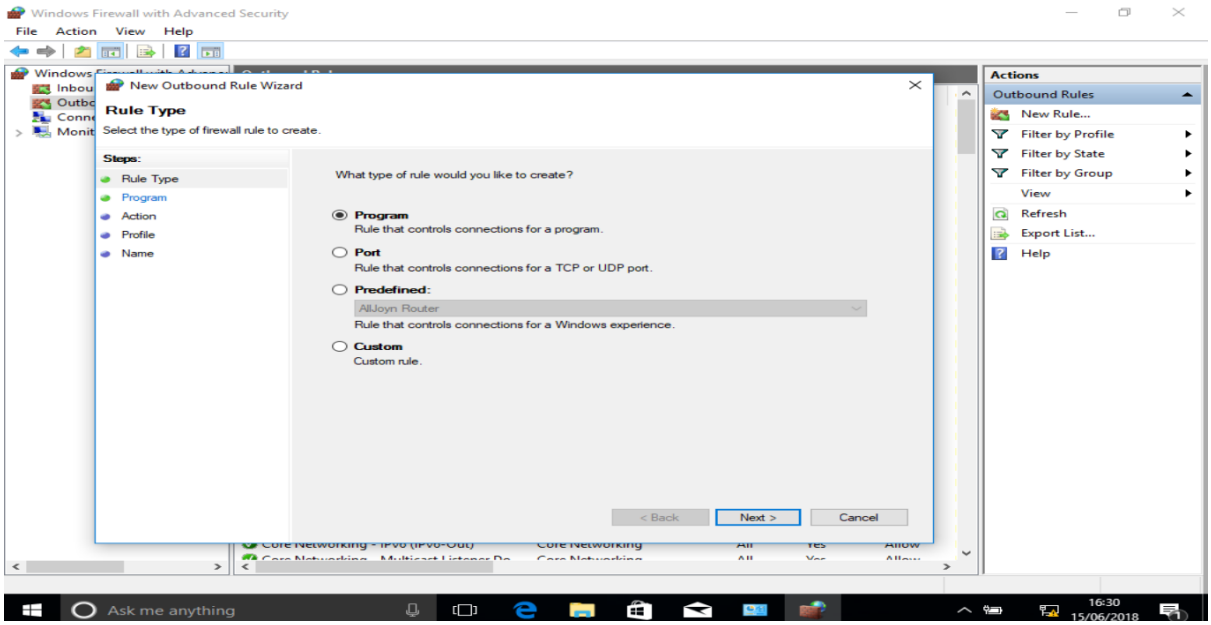
This screenshot shows me setting up a scheduled scan to happen every Monday at midnight.

I have done this so that the system automatically checks for files and this will avoid manual scans being forgotten. Therefore, this increases the amount of security on the system as even if the system is manually scanned there will be an automatic scan to make sure that the system is being kept safe.

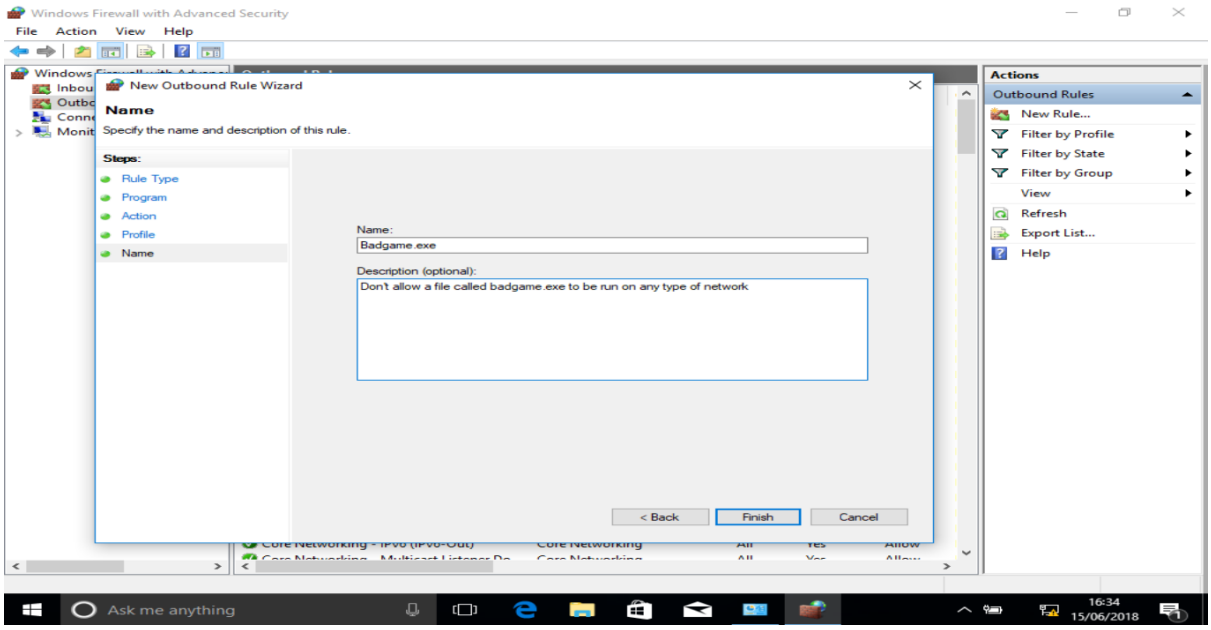
Firewall



The first screenshot shows that the firewall has been setup.



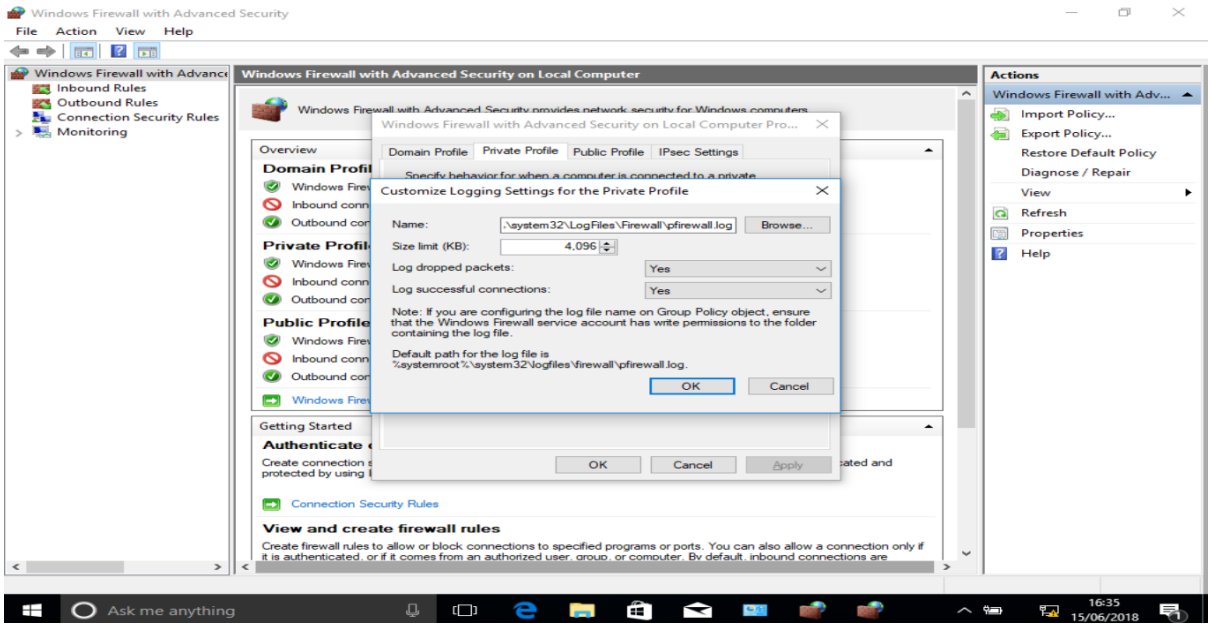
This screenshot is showing that I am setting up a condition for a program in the firewall.



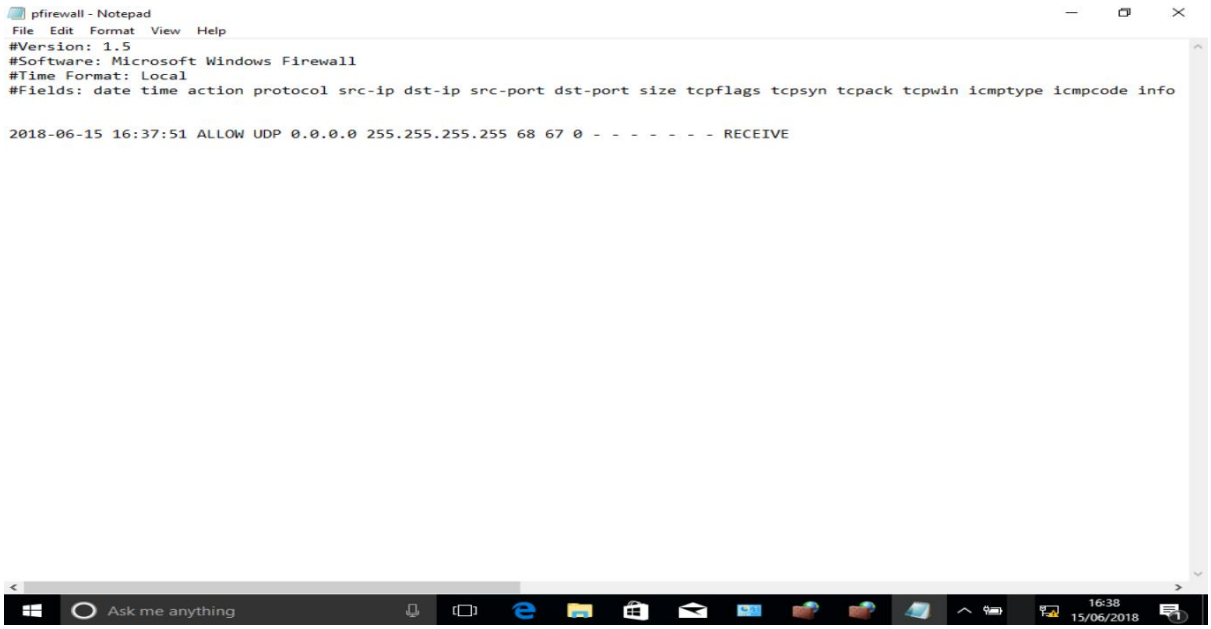
The above screenshot shows that I have made a condition to not allow any file called Badgame.exe to run.

I have set up Windows Firewall on the system so that files with certain names won't be able to be run. This could be adjusted so that all files of a certain type like .exe files won't be able to run on non-admin accounts. Therefore, it will stop non-authorised users from being able to put unwanted and potentially harmful applications from being put onto the system.

Firewall Logging



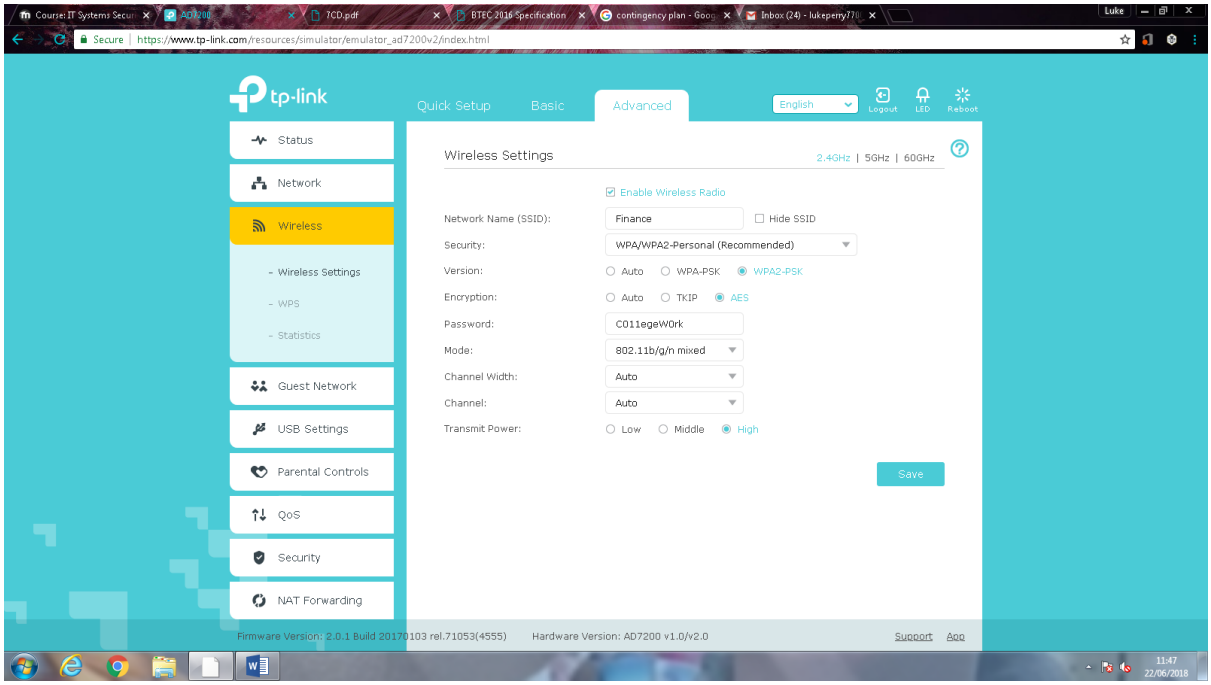
This screenshot shows me setting up the firewall event log so I will be able to see all the activity that takes place on the system.



This shows the event log in the firewall after I have given permission for a program to run.

This is effective because it will show the data, time, IP and what action has been done so if any suspicious activity is seen then it is clear on what machine has done it and what has been done so it should be possible to go back on any bad changes that may have taken place.

Wireless Security



This screenshot shows that I have set up the wireless security and have given the network a name, password and chosen the version it runs on and encryption type it uses. I chose to use WPA2-PSK as this uses AES algorithms automatically and has CCMP introduced with it making this version more secure than WPA-PSK. I also chose this version as the main vulnerability for this version is from an attacker that has access to the Wi-Fi so if anything does happen then it will most likely come from within the business. For encryption I have chosen AES over TKIP as TKIP isn't classed as a secure form of encryption anymore and AES is a lot more secure as it uses block ciphers. AES is also the modern standard for encryption as any vulnerabilities has been shown to be impractical or ineffective meaning that this should make the network as secure as it can get. With all the other security measures I have put into place it should allow admins to pin point where the attack is coming from and what files have been used in order to create the attack.

Testing

Test Number	Description	Expected Outcome	Actual Outcome
1	Check to see if the shared folder is accessible on other accounts	The shared folder can be viewed on all accounts on the system	The shared folder could be accessed on all the accounts
2	Check if control panel can be accessed by non-admins	Control panel should not be able to run on a non-admin account	Control panel couldn't be run
3	Check to see if the firewall is logging events correctly	When a program is allowed to run it should be logged in the log file	The action was logged in the firewall
4	Check to see if the anti-virus scans the system fully	The anti-virus should do a complete scan of the system and point out if any harmful files have been found	The anti-virus scanned the whole system and no harmful files were found
5	Check if a file called Badgame.exe is able to run	The firewall should stop the file being run	The firewall didn't allow the file Badgame.exe to be run

Feedback

Person 1

Q1: What do you think to the system that has been produced?

A1: I believe that the system manages to meet all the requirements and I trust that the software can start being used and financial transactions can take place.

Q2: What can be improved with the system?

A2: There could be an extra security measure of only allowing admins to run executable files so only trusted programs

Q3: What is good about the system?

A3: The security measures that have been put into place are really effective and work as intended.

Q4: Is the system easy to use?

A4: Yes

Person 2

Q1: What do you think to the system that has been produced?

A1: I think that the system is in a stable state that should be able to securely run the financial system

Q2: What can be improved with the system?

A2: With the financial software two factor authentication could be implemented to help better secure the accounts for the users

Q3: What is good about the system?

A3: There is many ways of protecting files and the network from being attacked that have been put in place

Q4: Is the system easy to use?

A4: Yes

Review

I believe that the system I have setup will protect the users very well by not allowing outside people to connect to the network and if an inside attack was to take place then the actions can be seen in the event log so it will be easy to track where the attack is coming from.

I have taken the feedback into consideration and in the future, I will add more security measures to make sure that only admins or trusted workers will have permission to run certain file types in order to avoid harmful applications or files from getting onto the system. I will also include a two-factor authentication option to allow users to have an option to give their account extra security.

However, the system has been setup as I intended and manages to secure the system fairly well. The use of group policies to stop certain workers from being able to access certain files and applications is really effective as, for example, it will stop people with no experience from damaging files that have code in them or vital parts of the software.