Thomas Robinson

Unit 5, Assignment 2

Managing a Network (Redacted Version)

Solihull College
November 2022
Redacted December 2022

Task One P5

College Network Interrogation

My PC

Using the *ipconfig* command, we can find out information about the computer and its configuration.

Image Redacted

Hostname

In the above screenshot taken from Windows Terminal, the first line reports the hostname (string used to identify the computer on the network) of the computer. In my case it is *REDACTED*.

IP Address

The IP Address of the computer is configured to be set dynamically using DHCP. Currently, the IP address of my PC is *REDACTED*. The DHCP server in use is *REDACTED* – more information about this will be acquired later.

Interrogating the Network

Interrogation is the process of obtaining information about the devices on a network and their configuration and details. This can include anything from network infrastructure such as routers, switches and servers to end devices such as printers and smartphones. Deeper interrogation into devices can discover running services through open ports as well as operating system version information using fingerprinting and other techniques.

Using Nmap

Nmap is an open-source command-line utility used for interrogating a network.

Zenmap is a GUI wrapper for the utility that provides a graphical output of an nmap scan.

Since the goal here is to interrogate the entire college network, I have chosen to run two scans of the subnets that are visible in the previous screenshot: *REDACTED/23* and *REDACTED/24*.

Image Redacted

Image: Using the Zenmap GUI for nmap to run a scan on two subnets at once.

Network Resources

DNS, DHCP & DC

The DHCP server of my local computer is *REDACTED*

Running a Traceroute to this address reveals the hostname is *REDACTED.solihull.ac.uk*—presumably standing for REDACTED.

Based on open ports, it REDACTED

Gateway

The Default Gateway as set by the DHCP server is *REDACTED*.

Visiting this IP in a web browser over the HTTPS protocol reveals REDACTED
The hostname of the device is uncoverable by viewing the certificate of the page: *REDACTED.solihull.ac.uk*. From this, we can infer REDACTED

Image Redacted

age Redact

REDACTED/24

REDACTED

Device Type	Approx Count
REDACTED	32
REDACTED	5
REDACTED	23
REDACTED	5

Image Redacted

REDACTED/23

REDACTED

Device Type	Approx Count
REDACTED	17
REDACTED	20
REDACTED	1
REDACTED	1

Image Redacted

Public IP

Image Redacted

To find the public IP address of the college network, we can use an Internet service that responds back with this information. In the above example, I am using PowerShell to invoke a web request to the *ipinfo.io* service. Using this we can see that the WAN address of the college router that served the request is *REDACTED*.

Further investigation into this IP address using the RIPE Network Coordination Centre website[1] in a browser reveals it is managed by AS787. This refers to the Autonomous System number of Jisc, a non-profit that provides IT services to educational and research institutions. Here, I also discover that the college (netname SOLIHULL-COL-UNI-CENTRE) has been allocated a /24 block of 255 public addresses from *212.219.7.0* to *212.219.7.255*.

[1] https://apps.db.ripe.net/db-web-ui/query?searchtext=REDACTED

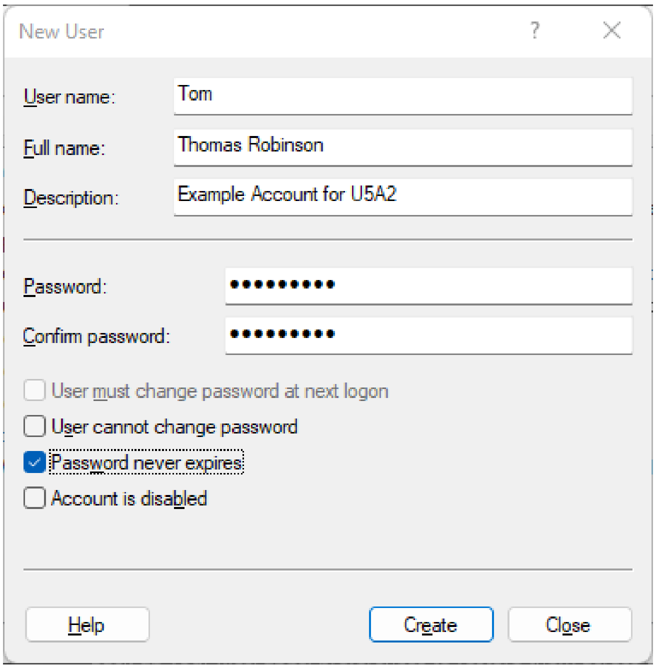
Task Two P6, M3

Network Management Tasks

User Account Creation 1st November 2022

As our user accounts do not have the appropriate permissions to create a new user from the Windows 11 Settings application, I will be using the Local Users and Groups utility. This accessible from within the Computer Management Application (compmgmt.msc) or as a standalone application (lusmgr.msc). Creation of users is an activity that should be undertaken whenever a new user account is required (for example: a new employee or student joins the organisation).

Image Redacted



New User

User name: Tom

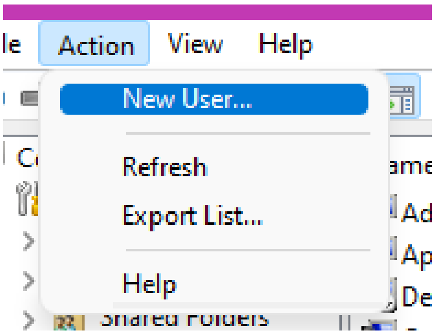
Full name: Thomas Robinson

Description: Example Account for U5A2

Password: •••••••••

Confirm password: •••••••••

☐ User must change password at next logon
☐ User cannot change password
☑ Password never expires
☐ Account is disabled



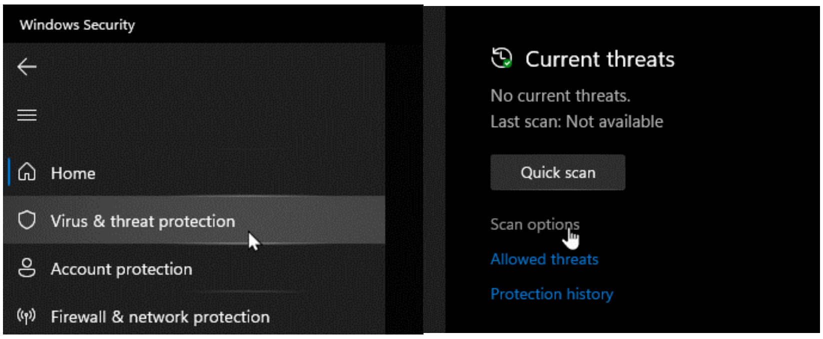
To create a new account, I selected "New User" from the action menu. The resulting dialog box allows us to set information such as the name of the user and setting an initial password.

Virus Scan 5th November 2022

Scanning for viruses on a regular basis ensures that no malicious software is on a machine. Modern versions of Windows include the Windows Security application that incorporates Windows Defender Antivirus. It can be configured to run scans on a regular basis or on-request. Smart App Control (formerly SmartScreen) is a feature that ensures the legitimacy of applications before they are opened.

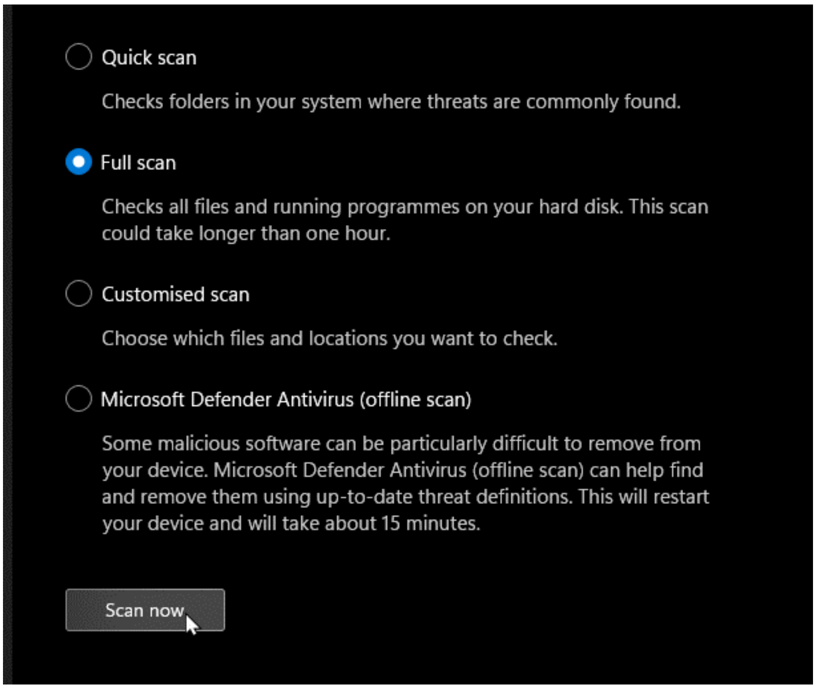
To run a manual scan with Windows Defender, I selected "Virus & threat protection" from the sidebar of the Windows Security application. After selecting "Scan options" I selected a full scan of the system.

Modern antivirus solutions can run real-time scans, which scan files when they are accessed or changed. Despite this, it is important to run thorough scans on a regular basis. Depending on the frequency of use that a system sees, or the importance of the data on said system, it could be advisable to run a scan anywhere from daily.



Current threats

No current threats.
Last scan: Not available



○ Quick scan

Checks folders in your system where threats are commonly found.

● Full scan

Checks all files and running programmes on your hard disk. This scan could take longer than one hour.

○ Customised scan

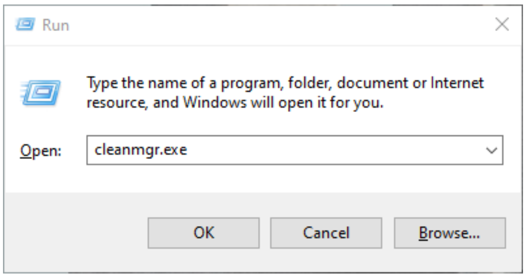
Choose which files and locations you want to check.

○ Microsoft Defender Antivirus (offline scan)

Some malicious software can be particularly difficult to remove from your device. Microsoft Defender Antivirus (offline scan) can help find and remove them using up-to-date threat definitions. This will restart your device and will take about 15 minutes.

File Clean-Up 1st November 2022

Windows contains a built-in utility for cleaning up temporary and unused files called Disk Clean-Up. It is accessible by searching in the Start Menu or by running *cleanmgr.exe*.

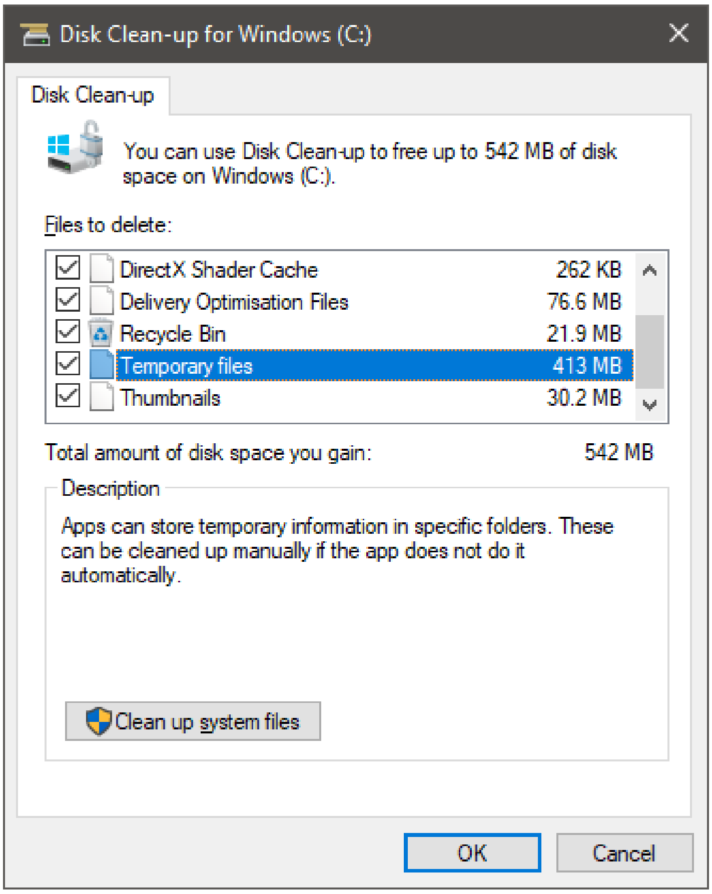

Run

Type the name of a program, folder, document or Internet resource, and Windows will open it for you.

Open: cleanmgr.exe

After a short time scanning the disk, a window appears describing what data can be deleted and the amount of space to be freed. Here, the largest source of used disk space is Temporary files from various applications which take up 413MB. With administrator privileges, it is possible to also clean-up system files such as the Windows Update download cache and previous Windows versions.

File clean ups should be run on a regular basis, such as every month, or whenever the need to free up some space arises.


Disk Clean-up for Windows (C:)

Disk Clean-up

You can use Disk Clean-up to free up to 542 MB of disk space on Windows (C:).

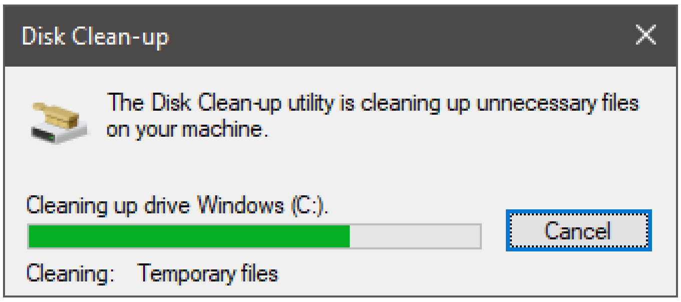
Files to delete:

☑	DirectX Shader Cache	262 KB
☑	Delivery Optimisation Files	76.6 MB
☑	Recycle Bin	21.9 MB
☑	Temporary files	413 MB
☑	Thumbnails	30.2 MB

Total amount of disk space you gain: 542 MB

Description

Apps can store temporary information in specific folders. These can be cleaned up manually if the app does not do it automatically.


Disk Clean-up

The Disk Clean-up utility is cleaning up unnecessary files on your machine.

Cleaning up drive Windows (C:).

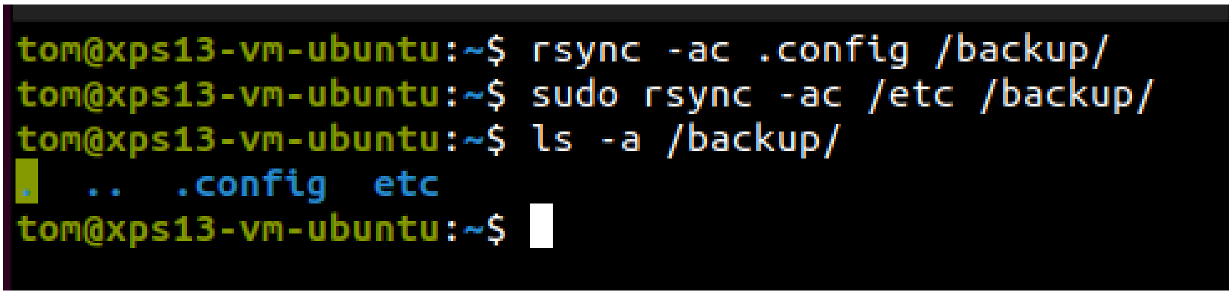
Cleaning: Temporary files

Configuration Backup 9th November 2022

In this example, we are backing up the configuration of a Linux machine running Ubuntu.

On Linux, most configuration data is stored in predicable locations. The */etc* folder stores systemwide configuration for services and applications and *~/.config* in a user's home folder is where user application settings are stored.

To backup this information, we are going to copy it to an external removable disk drive. To do this reliably, we can use the *rsync* program, which copies and verifies transferred data.



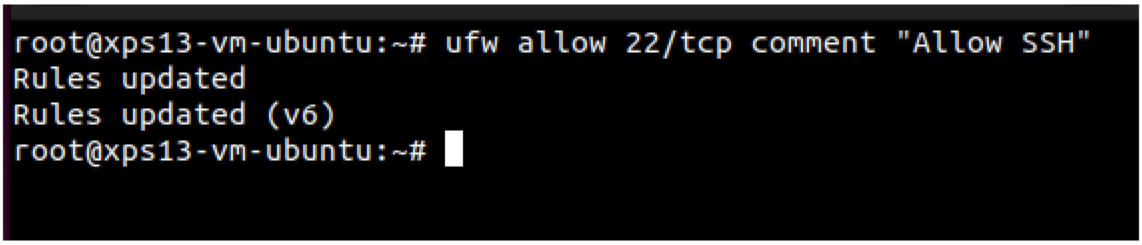
```
tom@xps13-vm-ubuntu:~$ rsync -ac .config /backup/
tom@xps13-vm-ubuntu:~$ sudo rsync -ac /etc /backup/
tom@xps13-vm-ubuntu:~$ ls -a /backup/
.  ..  .config  etc
tom@xps13-vm-ubuntu:~$ 
```

Backups should be made before and after major configuration changes to facilitate rolling back to previous versions should something go wrong.

Allowing SSH Access 10th November 2022

Client Computer

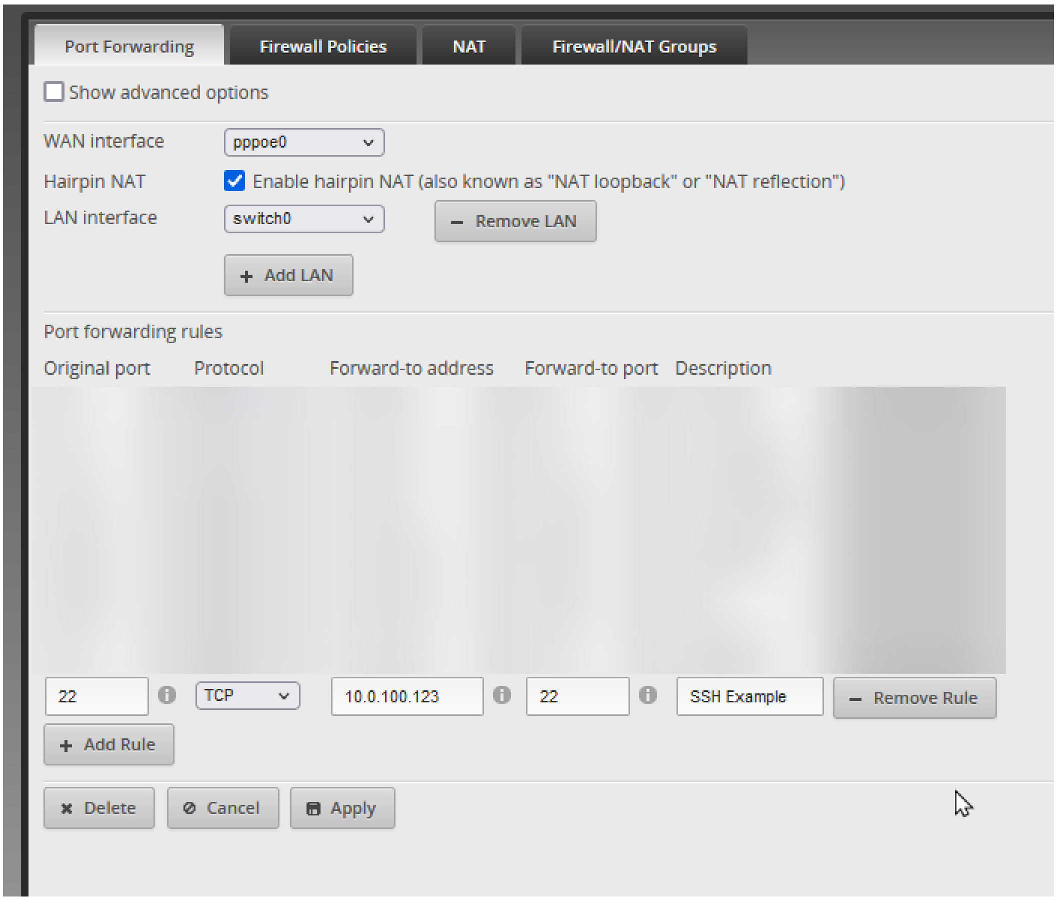
As SSH is primarily used on Linux systems, I am using Linux as the example here. On systems with *ufw* (uncomplicated firewall) installed, allowing SSH from other devices is as simple as running `ufw allow 22/tcp`. This allows connections through the local firewall on port 22 using the TCP protocol, the port and protocol that SSH uses.



```
root@xps13-vm-ubuntu:~# ufw allow 22/tcp comment "Allow SSH"
Rules updated
Rules updated (v6)
root@xps13-vm-ubuntu:~# 
```

Firewall

To allow access from outside the network, we can configure the network firewall. To allow access from the Internet, we can 'port forward' which opens a port on the firewall's WAN interface and packets sent to this port are forwarded to/from the specified address inside of the network.



□ Show advanced options

WAN interface: pppoe0

Hairpin NAT: ☑ Enable hairpin NAT (also known as "NAT loopback" or "NAT reflection")

LAN interface: switch0

Port forwarding rules

Original port	Protocol	Forward-to address	Forward-to port	Description
[redacted]				
22	TCP	10.0.100.123	22	SSH Example

Task Three D2

Network Security Policy

Scope & Purpose

The purpose of this document is to lay out steps that must be undertaken to keep the Organisation’s network functional and secure. It issues guidance that must be abided to by Staff and Students as well as Network Administrators, guests, and outside contractors.

Acceptable Use & Logging

Acceptable Use of the network covers resources that are forbidden from being accessed and activities that are prohibited.

Accessing content that does is not of educational merit or business use to the Organisation is forbidden. Under the Computer Misuse Act, knowingly gaining access to systems that one is unauthorised to access is against the law.

Performing actions that may significantly degrade the experience of other network users, such as excessive downloading of large files or attempts to probe or interrogate network hosts are disallowed without explicit permission from the IT Team.

When using the Organisation’s network, users should have no expectation of complete privacy and therefore should not engage in personal activities such as online banking.

Users of the network are reminded that all activity is actively monitored and logged for the purpose of prevention and detection. Users found to have accessed resources or in breach of the Acceptable Use Policy outlined above will be subject to appropriate disciplinary action.

Confidentiality & Data Protection

When using the Organisation’s network, it is important to ensure appropriate levels of data integrity and data security.

Under Data Protection Regulation, personally identifiable information (PII) is to be treated with the utmost respect. PII is not to be shared or distributed without prior permission from the Organisation’s appointed Data Protection Officer.

PII should not be kept for longer than is needed.

Documents and information marked as classified and confidential are not to be shared outside of the Organisation without prior permission.

Training

Users of the network will be subject to periodic training and guidance provided by the IT Team. Users are required to be knowledgeable about the risks and dangers that are posed when using the network as well as general security good practices.

Passwords & Accounts

It is expected that users keep their login details, including usernames and passwords, private. The sharing of user accounts or user login details is prohibited. Those without an account that require access to the Organisation’s network should raise an inquiry with the IT Helpdesk.

Passwords must contain the following in order to be secure:
- At least 8 characters in length
- Contains 1 or more digit
- Contains 1 or more special characters
- Does not contain sequential characters or digits
- Does not contain all or part of a username or other easily guessable information, such as a birthday or location.

All user accounts are additionally required to be enrolled in two-step verification. This could take the form of an SMS text message code, an authentication app or a physical hardware device.

BYOD & Working from Home

After the Covid-19 pandemic, the practice of working remotely where possible became more popular. It is the policy of the Organisation that remote work be subject to the same scrutiny as work within the Organisation’s buildings.

Personal devices used to access the Organisation’s information or the Organisation’s network are required to be kept up-to-date and with appropriate anti-malware software. Assistance with installing this is available from the IT Helpdesk if required.

When using the Organisation's VPN to access the network remotely, users are reminded of the acceptable use policy. This will apply to all use when connected to the Organisation's network, regardless of the device used.

Disaster Recovery

The Organisation employs numerous strategies to mitigate the risks of potential disasters that may occur.

User Data and data critical to the Organisation is backed up on a regular basis to multiple places, some off-site. In the event of a ransomware attack, hardware failure or other issue that primarily impacts data, the Organisation is well equipped to restore this information in a timely manner.

The Organisation maintains a replicated warm server rack located away from the main campus. Should a disaster, natural or otherwise, impact the primary servers, these can quickly be deployed as a fallback to allow the Organisation to continue work.

Should the buildings of the Organisation become inaccessible, it is expected that users work remotely when possible until alternative arrangements can be made.

Checking of User Access Rights

User Access Rights are the rules that dictate which User Accounts have access to perform certain activities, such as reading and writing data or accessing certain systems and applications. This policy also covers the deletion and pruning of unused or outdated accounts.

It is the responsibility of the Network Administrators to regularly undertake checks of the various ACL systems on the network to ensure that privileges for each account or user group are appropriate. For example, ensuring that a temporary guest user is unable to access student data.

It is the responsibility of the Network Administrators to check firewall rules between networks within the organisation and how they communicate with the internet.

It is the responsibility of the Network Administrators to regularly inspect the User Account Database and ensure that any unnecessary user accounts are deleted. Former employees and temporary testing accounts are examples of unnecessary accounts that should be pruned.

Penetration Testing

Penetration Testing is the process of checking the network and attempting to uncover vulnerabilities.

Testing should be carried out by a trusted third-party on a regular basis.