// Assignment 2

/ Managing a Network

// by George Hotten

// Interrogating the College Network

To get a list of all devices on my network, I will use a tool called Nmap. Using this, I can iterate through every possible IP address on the network to identify devices.

// My IP address

First, I will need to identify what my IP and subnet are. I can do this by running the following command in the terminal: ip config /all

nernet adapter Ethernet:
Connection-specific DNS Suffix . : solihull.ac.uk
Description Intel(R) Ethernet Connection (2) I219-V
Physical Address 2C-F0-5D-06-EC-64
DHCP Enabled Yes
Autoconfiguration Enabled : Yes
Link-local IPv6 Address : fe80::11d6:218a:5ac3:636f%4(Preferred)
IPv4 Address
Subnet Mask
Lease Obtained
Lease Expires
Default Gateway
DHCP Server
DHCPv6 IAID
DHCPv6 Client DUID
DNS Servers
192.168.224.101
NetBIOS over Tcpip : Enabled

From this, I can see my IP address is 172.20.52.109. Based off our subnet mask, the IP address we will input into Nmap to scan every possible IP address withing the network is 172.20.52.0/23.

/ Our Hostname

To identify our hostname, we can simply run the **hostname** command within command prompt.

C:\Users\Net 2>hostname DESKTOP-40Q4NU2

Our hostname is DESKTOP-40Q4NU2.

// Scanning the Network

To scan the network, and to obtain information about the type of device, we will use the following Nmap command: nmap -T4 -A -v 172.20.52.0/23. Let's break down what this means:

/ nmap – the application we are running

/ -T4 - set timing template

/ -A – enables OS detection, version detection, script scanning and tracert

/ -v - increases level of verbosity.

As some IP addresses from our IP config were from the subnet 192.168.224.0, I will run a scan on this too.

/ Devices on 172.20.52.0



This subnet generally consists of PCs, printers, and access points. Essential services such as DCHP and DNS are not found on this network, and devices must make 2 hops to reach the respective server. This subnet's router is located at 172.20.52.1.

Device Type	Amount
General Purpose	75
Printers	1
Networking	2
Servers	0

/ Devices on 192.168.224.0



On this subnet, devices consist mainly of servers including services such as DHCP, DNS, active directory and more. This subnet's router is located at 192.168.224.254.

From the above graph we can also see that the college's primary router to the outside world is located at 192.168.225.254.

Device Type	Amount
General Purpose	0
Printing	1
Networking	3
Servers	96

// Our public IP

Traci	ng route	to hotten	.uk [172	.67.175.41]
over	a maximum	of 30 ho	ps:	
1	<1 ms	<1 ms	<1 ms	172.20.52.1
2	<1 ms	<1 ms	<1 ms	212.219.7.1

Using tracert, I was able to identify that our public IP address is 212.219.7.1.

// Issues during the interrogation

One issue I found the accuracy of Nmap's OS detection to be poor. For example, throughout my scan of the 172.20.52.0 most computers were reported as running Windows XP Service Pack 3, whereas the computers are running Windows 10 and 11.

// Routine Management Tasks

Please note these tasks were performed on Windows Server 2022 and may not be applicable to other versions of Windows.

// Creating a new user

To create a new user, first we must open the Local Users and Groups snap-in. We can do this by using Run, by pressing Windows + R, then typing in lusrmgr.msc.

🖅 Run		Х	
٨	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.		
<u>O</u> pen:	Iusrmgr.msc ~ Itis task will be created with administrative privileges.		
	OK Cancel <u>B</u> rowse]	

This then opens the Local Users and Groups snap-in, to get to the menu we need, click on "Users" on the left hand side.



By right clicking and pressing the New User button we can add a new user.



t New User				?	×
User name:					
Full name:					
Description:					
Password:					
Confirm password:					
User must char	ge password at i	next logon			
User cannot ch	ange password				
Password neve	r expires				
Account is disa	bled				
Help		Cr	eate	Close	

Now I can fill in my details and created press Create.

New User		?	×
User name:	george		
Full name:	George Hotten		
Description:			
Password:	•••••		
Confirm passwo	rd:		
User must cl	hange password at next logon		
User cannot	change password		
Password ne	ever expires		
Account is d	lisabled		
Help	Create	e Clo	se

I have selected that my password never expires, however for more security this can be enabled.

Name	Full Name	Description
🛃 Administrator		Built-in account for administering
🛃 DefaultAcco		A user account managed by the s
🛃 george	George Hotten	
🛃 Guest		Built-in account for guest access t
🛃 WDAGUtility		A user account managed and use

My account is now created. I completed this on 02/11/22. New users can be added whenever they're needed. It is good practice to review your users to ensure details are up-to-date and only accounts that need to be active are active. This can be done every month.

// Running a virus scan

To run a virus scan, we must open the Windows security dashboard. We can access it by typing Windows Security into the search bar.

፼ <u></u> <u></u>		
Best match		
Windows Security		
Settings		
Windows Security settings		
Windows Security		
✓ Windows Security	Ħ 💽 肩	

After it opens, we can press Virus and Threat Protection and press Quick Scan.



😉 Current threats

Quick scan running... Estimated time remaining: 00:00:09 1134 files scanned

Cancel

Feel free to keep working while we scan your device.

Protection history

After the scan is completed, you will get a summary of the scan.



No current threats. Last scan: 11/2/2022 9:23 AM (quick scan) 0 threats found. Scan lasted 23 seconds 35053 files scanned.

This was completed on 02/11/22. A virus scan should at minimum be completed daily. It can be completed every few hours depending on the severity of the data stored on the device.

// File clean-up

To access the file clean-up utility, you can search Disk Cleanup into the search bar.



Windows will now scan your drives looking for any files that can be cleaned-up.



After this is completed, a summary of files will be shown, and you can choose what you want to be removed.

🖀 Disk Cleanup for System Drive (C:)		×
Disk Cleanup More Options		
You can use Disk Cleanup to free up to 26.7 space on System Drive (C:).	MB of disk	
<u>Files to delete:</u>		
Microsoft Defender Antivirus	1.03 MB	~
Downloaded Program Files	0 bytes	
🗹 🔒 Temporary Internet Files	25.2 KB	
Windows error reports and feedback di	6.35 KB	
DirectX Shader Cache	0 bytes	~
Total amount of disk space you gain:	26.7 M	1B
Description		
Non critical files used by Microsoft Defender Antivin	IS	
ОК	Can	cel

After pressing OK, the system will now start deleting the files selected.

Disk Cleanup	×
The Disk Cleanup utility is cleaning up unnecessary file on your machine.	s
Cleaning up drive System Drive (C:). Cancel	
Cleaning: Device driver packages	

The disk clean-up is now completed. This was completed on 02/11/22. This can be completed between every week and every month.

// Backup the configuration

To create a backup, first we must open the Windows Server Backup snap-in. This can be done by typing wbadmin.msc into Window's Run dialogue.

💷 Run		×
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.	
Open:	wbadmin.msc 🗸 🗸	
	This task will be created with administrative privileges.	
	OK Cancel Browse]

After the snap-in opens, press Local Back up on the right hand-side then press Backup Schedule.

1 1 1 1	Windows Server Backup (l 🏠 Local Backup
Acti	ions
Loc	al Backup 🔺
1	Backup Schedule
1	Backup Once
1	Recover
	Configure Performance Settings
	View 🕨
?	Help

After the wizard opens, select Custom Backup

🔥 Backup Schedule Wizard		×	ĺ
Select Back	up Configuration		
Getting Started Select Backup Configurat Select Items for Backup Specify Backup Time Specify Destination Type Confirmation Summary	 What type of configuration do you want to schedule? Full server (recommended) I want to back up all my server data, applications and system state. Backup size: 11.79 GB © Custom I want to choose custom volumes, files for backup. 		
	< Previous Next > Finish Cancel		

After continuing, select the following item to be backed up: C:\ProgramData and C:\Windows\System32\config. The config path contains the registry and other system configurations.

擾 Backup Schedule Wizard	×
Select Items	for Backup
Getting Started Select Backup Configurat Select Items for Backup Specify Backup Time Specify Destination Type Confirmation Summary	Select the items that you want to back up. Selecting bare metal recovery will provide you with the most options if you need to perform a recovery. Name C:\ProgramData C:\Windows\System32\config
	Add Items Remove Items Add Items Remove Items Advanced Settings Advanced Settings

After progressing, you can choose how often the data should be backed up. In this example, we will run the backup every day at 9PM, however it can be run as often as every half-hour.

5 🍖 Backup Schedule Wizard		×
Specify Bac	kup Time	
Getting Started	How often and when do you want to run backups?	
Select Backup Configurat	Once a day	
Select Items for Backup	Select time of day: 9:00 PM V	
Specify Backup Time	O More than once a day	
Specify Destination Type	Click an available time and then click Add to add it to the backup schedule.	
Confirmation	Available time: Scheduled time:	
Summary	12:00 AM 12:30 AM 1:00 AM 1:30 AM 2:00 AM 2:30 AM 3:00 AM 3:00 AM 3:00 AM 3:00 AM	
	4:30 AM V < Previous Next > Finish Cancel]

Now you can choose where the back-up is stored to. A separate drive is recommended, however for this demo I will use a volume I partitioned.

or 🍖 Backup Schedule Wizard		×
Specify Des	tination Type	
Getting Started Select Backup Configurat Select Items for Backup Specify Backup Time Specify Destination Type Select Destination Volume Confirmation Summary	 Where do you want to store the backups? Back up to a hard disk that is dedicated for backups (recommended) Choose this option for the safest way to store backups. The hard disk that you use will be formatted and then dedicated to only store backups. Back up to a volume Choose this option if you cannot dedicate an entire disk for backups. Note that the performance of the volume may be reduced by up to 200 percent while it is used to store backups. We recommend that you do not store other server data on the same volume. Back up to a shared network folder Choose this option if you do not want to store backups locally on the server. Note that you will only have one backup at a time because when you create a new backup it overwrites the previous backup. 	e e
	< Previous Next > Finish Cancel	

I will now select the volume I want my backups to be stored to.

» 🍖 E	ackup Schedule Wizard				×
	Select Desti	nation Volume			
Get Sele	ting Started ect Backup Configurat	Select one or more volum disks if you want to store l	es to store your backup backups offsite.	os. Use multip	ble volumes in different
Sele	ect Items for Backup	Volume	Disk	Capacity	Free Space
Spe	cify Backup Time	Backups (B:)	Red Hat VirtIO SC	10.00 GB	9.96 GB
Spe Sele Cor Sun	cify Destination Type ect Destination Volume firmation nmary				
		< Previou	s Nevt s	Finish	Add Remove
		< Previou	s Next >	Finish	Cancel

Finally, after confirming everything is correct, we can finish the setup.

Confirmatio					
	on				
Getting Started Select Backup Configurat Select Items for Backup Specify Backup Time Specify Destination Type Select Destination Volume Confirmation Summary	You are about to cr Backup times: Files excluded: Advanced option: Backup destination Name Backups (B:)	eate the follow 9:00 PM None VSS Copy ns Size 10.00 GB	ving backup scher Backup Used Space 37.15 MB	dule.	
	Backup items Name C:\Progra C:\Window	mData ws\System32\	config	Einish	Cancel

Scheduled Backup				
A regular scheduled	backup is configured for this server			
Settings		Dest	ination usage –	
Backup items:	Selected files (System Drive (C:))	Nam	ne:	Backups (B:)
File excluded:	None	Can	acity:	10.00 GB
Advanced option:	VSS Copy Backup	User	d snace:	0 GB
Destination:	Backups (B:)	Back	kups available:	0 copies
Backup time:	Every day 9:00 PM		10 1.1.1	
			view details	
		-	Refresh inforr	nation

Our schedule is now created. This was completed on 02/11/22. Backups should be completed on a regular basis in line with the importance of data stored. For example, critical data could be backed up every hour whilst a user's program data could be backed up weekly.

// Enabling SSH and configuring the firewall

To start, navigate to Settings, Apps, Optional Features.

From there,	select Add	Feature	and type	in Open	SSH an	nd install	the server.
				•			

~	Add an optional feature	
命	Open \wp	
	Sort by: Name 🗸	
+	OpenSSH Server 1.33 MB	
See o	OpenSSH-based secure shell (SSH) server, for secure key management and access from remote machines.	
Insta		
Find		
Sort k		
¢		
ረን		
¢		
₹3	Install (1) Cancel	

Latest actions



OpenSSH automatically configures the firewall for us. Let's check it. We can access the firewall settings by typing wf.msc into the Window's Run dialogue.



After the snap-in opens, select Inbound Rules and search for OpenSSH SSH Server.

Intound Nules
Name Group ^ Profile Enabled Action Override Program Local Address Remote Address Protocol Local Port Remote Port Authorized Users A tub (²)OpenSSH SSH Server (sthd) OpenSSH Server All Yes Allow No %System... Any Any TCP 22 Any Any Any Any

As we can see, this inbound rule is configured to allow traffic from port 22 over the TCP protocol allowing SSH to function.

This was completed on 02/11/22. This does not need to be repeated; however it is good practice to check your firewall every week to ensure all policies are recognised and correct.

// Network Security Policy

// Acceptable Usage Policy

Before using the network, all users should agree to a network acceptable usage policy (AUP). An AUP should contain what is and isn't allowed on the network. Typically, this contains not sharing your login details, following password complexity requirements, and not tampering with any computer or network settings. AUPs also outline the disciplinary action that will be taken if the policy is broken, such as verbal/written warnings or the blocking of your network access.

// Responsibilities

All network users are responsible for ensuring that they follow the appropriate training and best practices whilst using the network. For example, not clicking any suspicious links in e-mails or downloading files from an untrusted source.

// User Access Rights

Users of the network should only have access rights for what is required to complete their job. For example, people in the training department would not need access to the business' financial records. This is essentially important if an account is compromised, if the account has proper access rights set the damage will be minimised as they won't have access to everything within the network.

/ Timing for Reviews

User Access Rights should be reviewed every 3 months and should be reviewed when operating systems are updated to ensure no changes have been made and any new policies can be configured.

// Firewall Rules

With threats constantly evolving, it is important to keep an up-to-date firewall to ensure that nothing malicious can enter the network. Firewalls allows a network administrator to chose what is allowed in and out of their network based on port numbers, packet filtering and TCP connection and session observation.

/ Timing for Reviews

Firewalls should ideally be reviewed every month inline with current threat information to ensure any emerging threats and malware can be blocked before they have the chance to cause any damage.

// Security Audits

Security Audits are usually untaken by a third-party who check the network's security configuration to ensure the current security strategy is adequate, proper training is being delivered and if any vulnerabilities are present. Once the security audit is finished, a list of priorities if created for any issues found and the fixes should be implemented in that order. The results of the security audit should be shared with any pre-determined parties.

/ Penetration Testing

During security audits, a penetration tester will attempt to breach your network to identify any vulnerabilities that are yet to be patched. The tester will deliver a final report to the network administrator or security auditor with details of any vulnerabilities found and how they can be patched.

// Scope

The scope of the security policy should be staff and guests who use the network's IT equipment and services.