Computer Networks

Assignment 3

Unit 9

George Hotten

Network Services

Directory Services

User Account Management

User accounts are often considered the backbone of network administration. User accounts management allows you to dictate who can access your network and what permissions they have (what they can and can't access, such as file shares). UAC also allows for you to manage logon hours and it can allow you to easily remove accounts that no longer need access to the network. Some other areas it can manage are:

- Password and requirements
- Contact information
- Home directory
- Group policy

Active Directory

Active Directory is a database management system that can control and keep track of all compatible devices on a network and allows data to sync between them. For example, network users can log into any device that is part of the 'domain' (a unit for grouping related objects) and have all their data synced across. Active Directory has built in user management (like above), device management, group policies for restrictions and much more.

Domain Name System

A DNS server can convert a URL to an IP Address so the computer can access the specific website. For example, when you enter 'google.com' into your browser it makes a request to a DNS server which then retrieves the correct IP and sends it back to the browser. For example, '216.239.51.100'. The browser then uses that IP to send the request to the web server.

Telecommunication Services

E-mail

E-mail is a method of communication using text and images. This allows people to easily collaborate and share information with other people. For e-mail to work, it requires a mail server. When sending an e-mail, your e-mail client makes a request to the e-mail server via Simple Mail Transfer Protocol. Once the e-mail server receives it, it is sent to the recipient via Internet Message Access Protocol (or Post Office Protocol, but that is out-of-date). Whilst this seems simple, there is a lot of other tasks going ahead on the mail server that the end user doesn't know about. For example, the mail server filters spam and virus emails, flags potentially dangerous or misleading emails, processes attachments, processes calendar events and account information, along with managing the end users' folders and inboxes.

Forums

Forums are online discussion boards where everyone can talk to each other (via text) about different topics in what is called a 'thread', which houses messages about a specific topic. Anyone can sign up to a forum and all data is stored centrally on one server. All messages can be accessed by everyone, including accessing messages from years in the past. Forums often have moderators who read through all messages, filtering out any spam or anything malicious.

Remote Desktop

Remote Desktop allows system administrators to access a computer from another location. For example, they could access their work computer from home. No extra configuration is required as Windows comes with RDP built in. This allows you to access all your files on that computer, transfer files to and from the computer, remotely monitor the network, and allows for security configuration to allow or disallow certain users from access the machine.

Social Networking

As social networking increases in popularity, businesses may want to create their own network so employees can talk to each other, access shared files and useful information. This can be setup by getting a dedicated server for the hosting and running of the network at the backend, and a front-end user interface so the users can interact with the system. There should also be tools to allow the users to customise their profile and their space.

Voice over Internet Protocol

VoIP converts your voice into a digital signal so you can make calls over the internet using the Internet Protocol. Once the voice data is received, it is converted back into sound and is played to the recipient's speaker. Data is sent via the typical method of packet switching.

File Services

File Transfer Protocol

File Transfer Protocol, FTP, is the protocol used to send and receive files between two computers over a network and/or the internet.

File Sharing

File Sharing is often done via network shares on the SMB (Server Message Block) protocol. Network shares allow for administrators to setup folders that can be accessed by specified people within a network. Each group / user can be setup with specific permissions, such as read or read-write. The network share is often hosted on dedicated file servers such as a NAS (Network Attached Storage). Having network drives allows for users within a network to collaborate and share files with ease.

Application Services

Databases

Databases are structures of data stored on a database server such as Microsoft's SQL server, or MySQL. Databases are used to hold data for specific services. For example, the database for a HR department would include all data relevant to them, such as employee information like name, age, wage, etc.

Web

A web server is a service on a server that responds to HTTP(S) requests, usually on port 80. When the server receives the request, it sends a response back (using HTTP(S)) with the desired information, such as a web page. Popular choices for a web server are Apache, NGINX, and Windows IIS. Web servers should monitor traffic, filter sites, send and receive requests and allocate the search results to the correct client.

Proxy

A proxy is a server that acts as a middleman when a client makes a request to a server. When a request is made, the packets of the request get sent to the proxy which decides if it should be forwarded to the intended server. Proxies perform tasks such as being a firewall by filtering out any malicious requests from the internet, filtering inappropriate web content and caching for frequently

accessed websites. Proxies can also have extra privacy features baked in, such as changing the IP address when the request to the actual server is made to protect the identity of the requester.

Shared Resources – Printers

Nowadays printers can be easily setup to connect to a network via their own built-in interfaces. Once it is connected to an access point within the network, anyone connected can use it. Before this, the printer would have to be directly connected to the central server or router. However, even if you don't directly connect it to a server, you should still manage it via the server so it can log the print requests and it will be able to make a more extensive print queue handling many more concurrent requests. This means even if the printer shuts down, all print jobs are saved until it turns back on. Having the printer managed by a server also allows an administrator to implement print restrictions and require funds for each job.

Shared Resources – Storage Space

Most networks have servers dedicated to providing extra, shared and accessible-anywhere storage. This allows users to store data on a 'network share' which will be available on any device on the network they log into. These servers are known as a NAS, aka Network Attached Storage. This further allows for multiple shares for different groups. For example, the administrators might have their own share for storing configuration files which normal users cannot access. Having network storage space also allows for centralised backups and they can be easily upgraded without having to service every device on the network.

The Usefulness of Directory Services

Account Management

Account management is useful as it allows for the centralised management of accounts across an entire network, thus allowing users to access their account from anywhere in the network. Account management is especially useful in the following:

User Profiles

ACM (Account Management) allows for IT administrators to setup user profiles for everyone on a network, with their own tailored roles and permissions. This means IT admins can allow, for example, certain users to perform certain tasks, whilst hiding the option from others.

Centralised Storage

ACM further allows for IT admins to setup network shares for users to access wherever they want within a network. Users can store their files on one machine and have them sync up on every other machine on the network. IT admins can set permissions on these shares to allow only certain users to access them, or setup read/write permissions so some users can only read not write to the shares.

Authentication Management

Authentication management is useful as it allows for users to access their account and all their data anywhere within the network. Sometimes even outside of the on-prem network via services such as Azure AD.

Logon Rules

AUC (Authentication Management) allows for IT admins to setup logon rules for different users. This includes setting allowed logon hours, meaning the user can only log into the network at set specific times. They can also restrict what machines users can and can't log into. This can further tie into

logon times as IT admins can set what machine users can log into AND the time they are allowed to log in.

Network Logon

Continuing from logon rules, users can logon to any machine that is connected to the organisation's active directory server. When the user tries to login, the computer makes a request to the AD server which checks the inputted username and password. If the details are valid, it returns the user's information needed to sign in and to setup their local account.

OAuth

OAuth, also known as Open Authorization, is the standard for access delegation that allows for users to log into a service using another account without giving their password [1]. This allows users to use one account for everything without needing to sign up for multiple services. This can be setup with Azure AD using an office login. Users can 'Login with Office 365' and have their details and user account synced to the service they want to access, whilst only giving data they consent to sharing.

Active Directory

Active Directory (AD) is useful as it allows for the centralised management of users, computers and devices such as printers and permissions.

Centralised Management

AD allows you to manage and sync settings to devices across a network connected to it. For example, AD manages all the users on a network, all the devices and all the permissions. All this can be managed in a single place, the AD Server Manage dashboard. AD allows for extensive permissions through Window's Group Policy (GP). GP has thousands of different policies that it allows you to configure, from disallowing certain features in a browser to changing the right-click menu.

Shared Devices

AD further allows you to extend your control over devices through its built-in services such as Printer Management. Printer Management allows IT admins to connect a printer to the AD server and then use the AD server as a print server. This means if the printer ever goes down, the queue will not be lost, and it allows for all devices connected to AD to print to the device. Linking back to centralised management, IT admins can control print permissions for the device and only allow select users to print to it if they so desire.

Domain Name System (DNS)

DNS is useful as it helps simplify the accessing of websites and services. Instead of remembering an IP address, users can remember a string called a URL instead. [2]

Easier to Remember

DNS allows you to remember a Uniform Resource Locator (URL) such as google.com, instead of 23.125.66.97 when trying to access a webpage. This makes it more convenient for users as remembering a few words is much easier than a string of numbers. This is especially useful if the webpage uses an IPv6 address.

Easier Web Management

DNS allows web admins to be much more flexible with their services. This is because if the IP of their web server needs to be changed, they can easily update their DNS record, and everyone will be able to use the webpage as normal. Without this, users would need to memorise a new IP address.

Sources

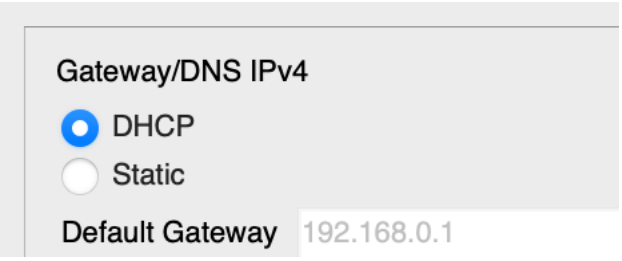
[1] https://en.wikipedia.org/wiki/OAuth

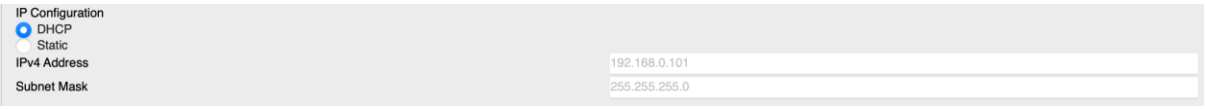
[2] https://www.cloudflare.com/en-gb/learning/dns/what-is-dns/

Making a Network Secure

Task 1

Turning on DHCP for PC0, then pinging the server.

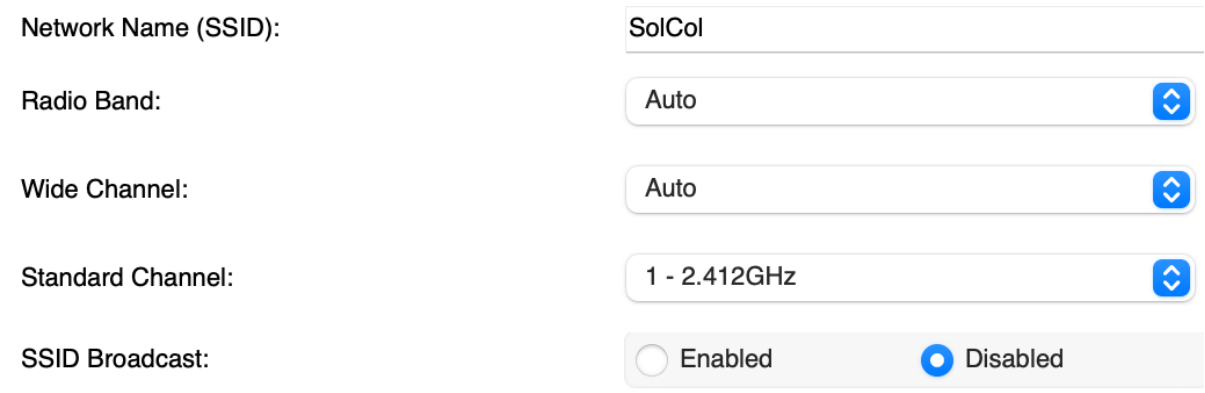





```
C:\>ping 192.168.0.102

Pinging 192.168.0.102 with 32 bytes of data:

Reply from 192.168.0.102: bytes=32 time=32ms TTL=128
Reply from 192.168.0.102: bytes=32 time=12ms TTL=128
Reply from 192.168.0.102: bytes=32 time=13ms TTL=128
Reply from 192.168.0.102: bytes=32 time=12ms TTL=128

Ping statistics for 192.168.0.102:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 32ms, Average = 17ms
```

Task 2

Setting the SSID to SolCol and disabling SSID broadcasting.



Task 3

Adding WPA2-PSK password encryption and setting the password to SolCol15.

Task 4

Connecting the two PCs to the wireless network.

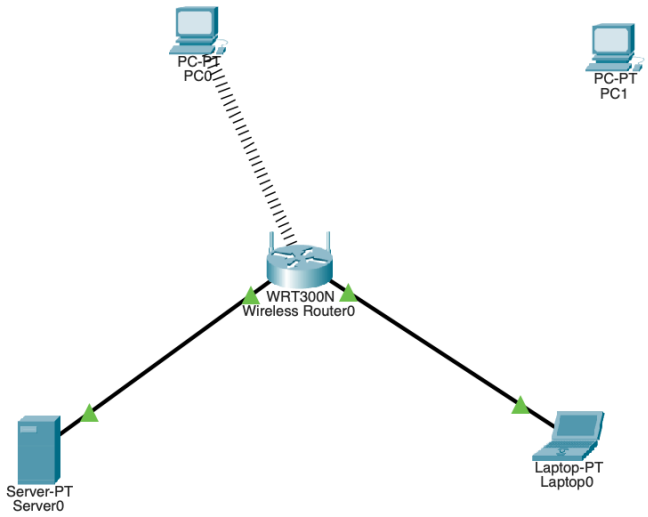
Task 5

Getting PC0's MAC address to add it to the access filter.

Turning on the MAC filter and adding PC0.

Task 6

Here is the final network:



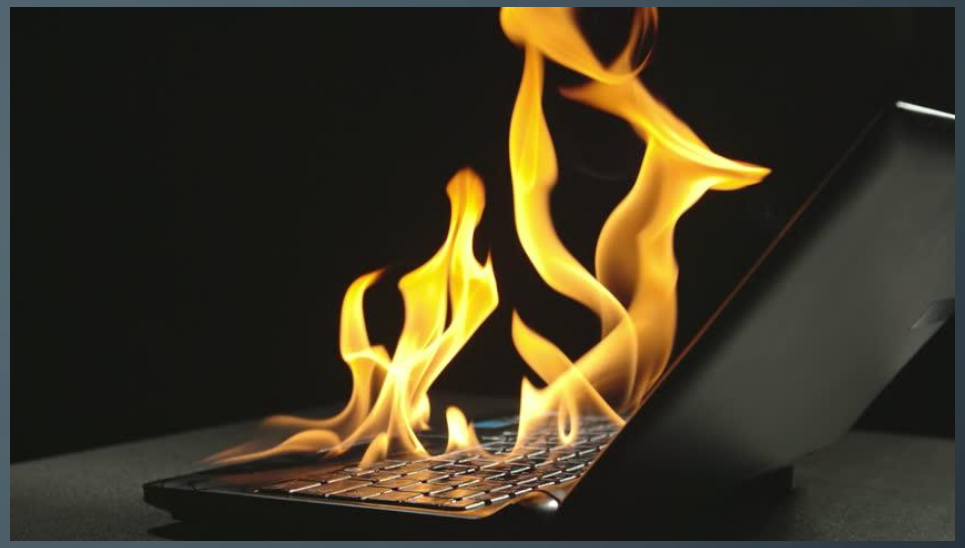
THE RISKS OF AN INSECURE NETWORK

BY GEORGE HOTTEN

THREATS TO A NETWORK

Theft / Malicious Damage

- Physical damage can occur via numerous means. Some intentional, some not.
- For example:
  - Damage from natural causes such as fires, earthquakes and floods.
  - Damage from vandalism.
  - Items being stolen.



Viruses

- Viruses are malicious software that aim to steal data or destroy a system. They can be transmitted via the internet or via physical means such as a USB stick.
- Some examples of viruses are:
  - Trojan – a virus that pretends to be something else.
  - Worm – a virus that spreads over a network.
  - Spyware – a virus that spies on a user's activities, key strokes, etc.

Remote Access

- Remote access is where hackers remotely access a computer or server in your network, with the intent to steal data or to damage the computer system.
- These systems are often able to be accessed due to misconfigured firewalls and network settings.

MITIGATING THE THREATS

Physical Security

- To prevent physical damage, the proper physical security measures should be taken. This includes having:
  - **Locks** – Locks can keep areas secure as they can prevent unauthorized people from entering them, for example where servers are. They must have the correct key to open the door to access the room. Only people who are authorized to interact with the servers should have a key. If one gets lost: all keys should be revoked, the locks changed, and new keys given. This also applies to RFID locks, which use special data encoded onto fobs or key cards to allow access.
  - **Biometrics** – Biometrics is using part of your body to authenticate you are really who you say you are. This could be done by verifying the person's fingerprint, face, voice, retina, etc. This adds an extra layer of security to prevent any impersonation or attempt to access someone else's data.
  - Other measures include: CCTV, barbed wire, exploding dye, alarms and guards.

User Account Security

- When securing a system from attacks, you want to ensure your user accounts are well protected.
- This is done by ensuring users only have access to what they need to, and enforcing a secure password policy with adequate multi-factor authentication in-place.

Software Security

- Software security is ensuring that all devices on your network are protected from software based attacks.
- Devices can be protected using: anti-viruses to block any malicious programs, application plugins such as adblockers or DNS sinkholes to protect from malicious adverts and program isolation (sandboxing) when running new programs to check for malware.

Network Intrusion Security

- Network intrusion security is ensuring no hackers can enter your network.
- Methods to protect from this include: firewalls to block unneeded ports and to deny access outside of the network or using an Intruder Detection System which analyses all data flowing through a network to check for any sign of intrusion based on the packet's metadata and content.
- Honey potting can also be used to attract hackers to meaningless data rather than your important files.