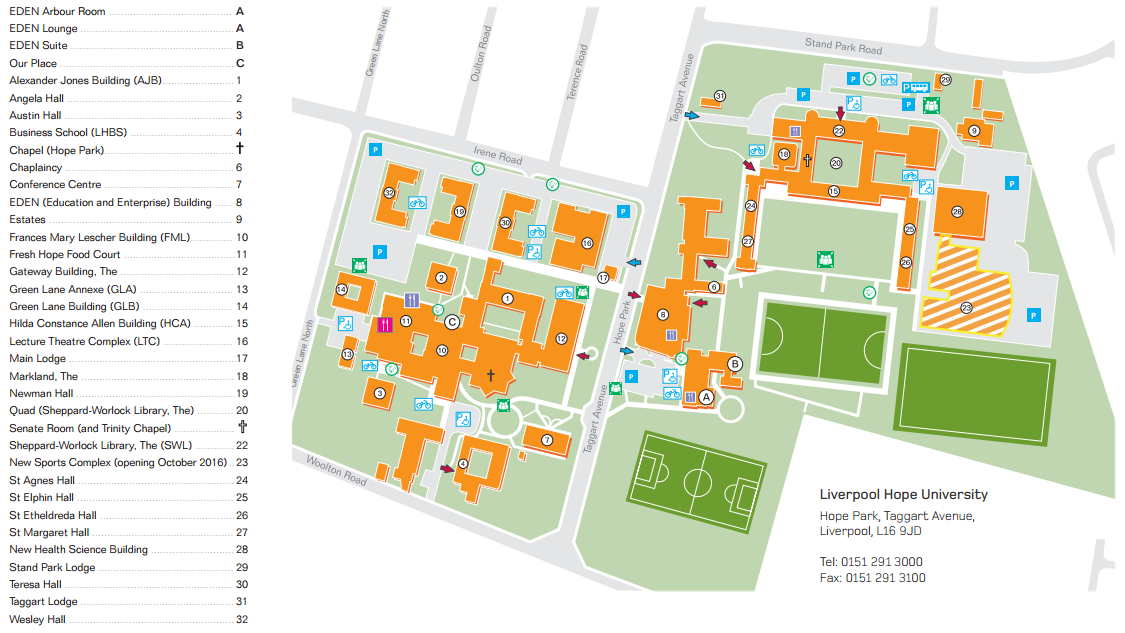
COM2057 Networks and Systems Administration ICA 1

Design of a Secure Campus Wireless Network



Madan Thapa

Q5030168

Introduction

We have to design a secure wireless network for the campus of Liverpool Hope University.

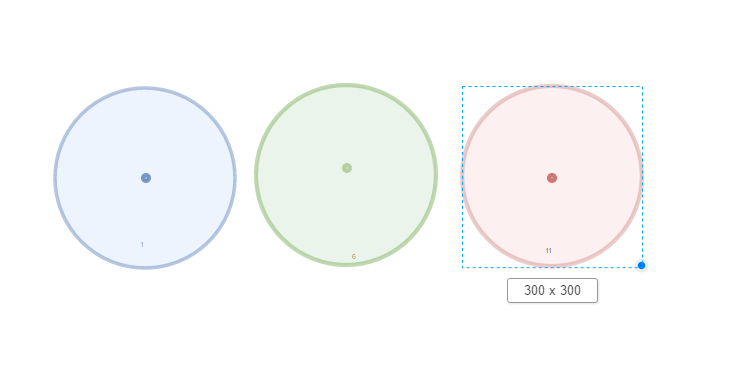
Task 1

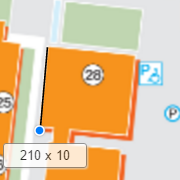
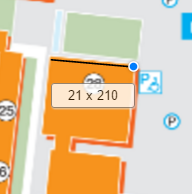
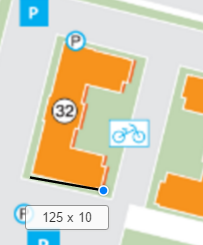
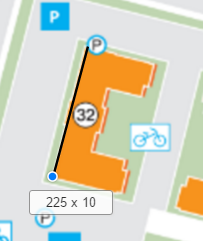
Get the buildings dimension of all the numbered buildings form 1-32, along with the number of floors and the occupancy for each of the buildings. I have based the occupancy on the size of the buildings, their functionality of the buildings, as I believe is halls are mostly busy, due to constantly having Students living there, along with cafes and library as every one form all the courses are coming in there, whereas others don’t get the occupancy as there is only people from that courses.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Building name | dimensions Length x Width(meters) | Floor (ground floor = 1 and 1st floor = 2) | Occupancy (0-100 = low, 100-500 = medium and 500+ high) |
| 1 | Alexander Jones Building (AJB) | 47 x 47 | 2 | Medium |
| 2 | Angela Hall | 20 x 18 | 4 | High |
| 3 | Austin Hall | 19 x 18 | 4 | High |
| 4 | Business School (LHBS | 31 x 43 | 2 | Low |
| 5 | Chapel (Hope Park) | 32 x 44 | 1 | Low |
| 6 | Chaplaincy | 46 x 9 | 1 | Low |
| 7 | Conference Centre | 32 x 16 | 1 | High |
| 8 | EDEN (Education and Enterprise) Building | 50 x 32 | 2 | High |
| 9 | Estates | 34 x 40 | 1 | Low |
| 10 | Frances Mary Lescher Building (FML | 50 x 38 | 4 | Medium |
| 11 | Fresh Hope Food Court | 42 x 30 | 1 | High |
| 12 | Gateway Building, The | 45 x 20 | 3 | High |
| 13 | Green Lane Annexe (GLA) | 20 x 8 | 2 | Low |
| 14 | Green Lane Building (GLB) | 20 x 25 | 2 | Low |
| 15 | Hilda Constance Allen Building (HCA) | 45 x 10 | 3 | Medium |
| 16 | Lecture Theatre Complex (LTC) | 42 x 35 | 1 | Medium |
| 17 | Main Lodge | 10 x 10 | 1 | Medium |
| 18 | Markland, The | 17 x 17 | 2 | Medium |
| 19 | Newman Hall | 45 x 25 | 4 | High |
| 20 | Quad (Sheppard-Worlock Library, The) | 32 x 32 | 3 | High |
| 21 | Senate Room (and Trinity Chapel) | 35 x 10 | 1 | Low |
| 22 | Sheppard-Worlock Library, The (SWL) | 52 x 16 | 2 | High |
| 23 | New Sports Complex | 53 x 57 | 1 | High |
| 24 | St Agnes Hall | 37 x 5 | 3 | High |
| 25 | St Elphin Hall | 37 x 5 | 3 | High |
| 26 | St Etheldreda Hall | 37 x 5 | 3 | High |
| 27 | St Margaret Hall | 37 x 5 | 3 | High |
| 28 | New Health Science Building | 42 x 42 | 1 | Low |
| 29 | Stand Park Lodge | 25 x 10 | 2 | Medium |
| 30 | Teresa Hall | 45 x 25 | 4 | High |
| 31 | Taggart Lodge | 17 x 7 | 2 | Medium |
| 32 | Wesley Hall | 45 x 25 | 4 | High |

Task 2

My scaling is 1m = 5pt. I used mostly 3 channels that are color coded. Blue = channel 1, Green = Channel 6, Red = Channel 11. I did however need to use one extra channel that was need on the building 13 and it was colored Yellow and channel 3, I choose this channel because it mixed with the channel 11 more than it did with channel 1 so the channel different will be more and there for less conflicted. I split the pics into 2 parts, they are scaled to this size. The WI-FI range get to ever building and none of them overlap more than 20%. They do how ever get into the car park, and I do have countermeasure for that.





Left

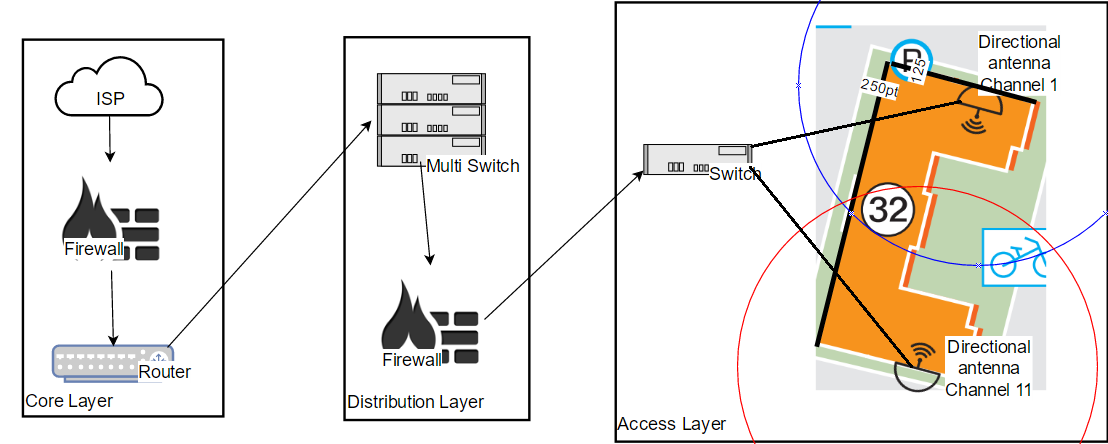
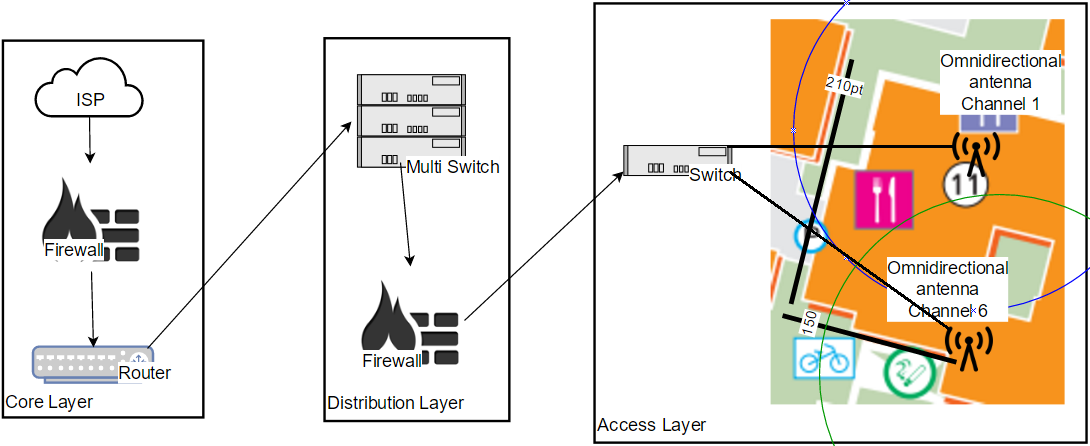
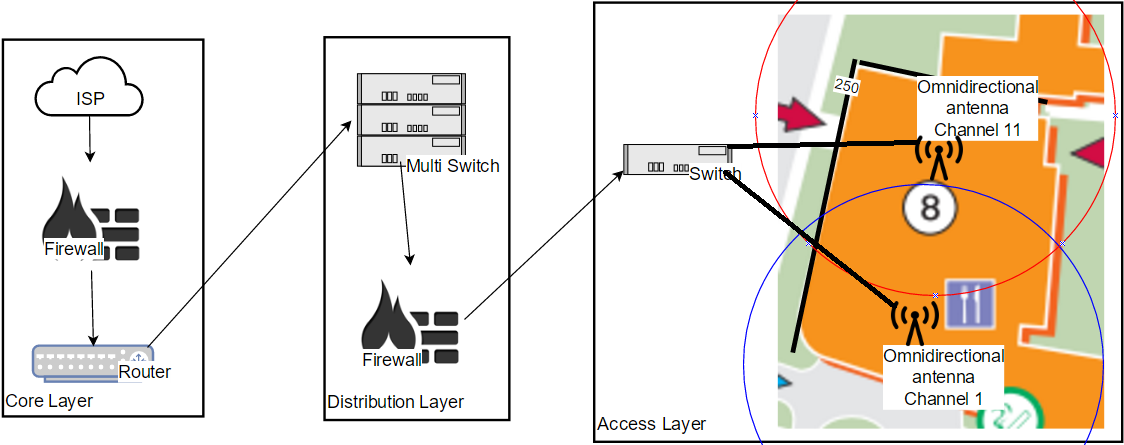


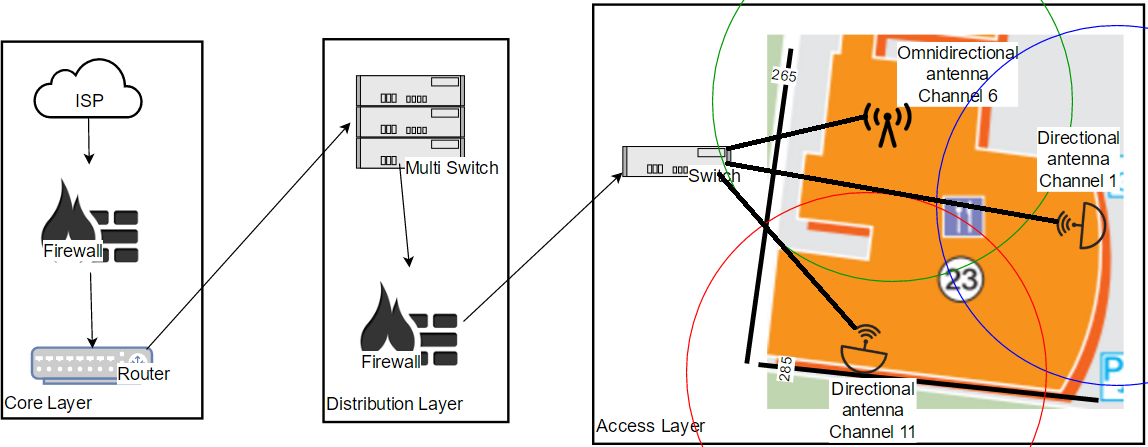
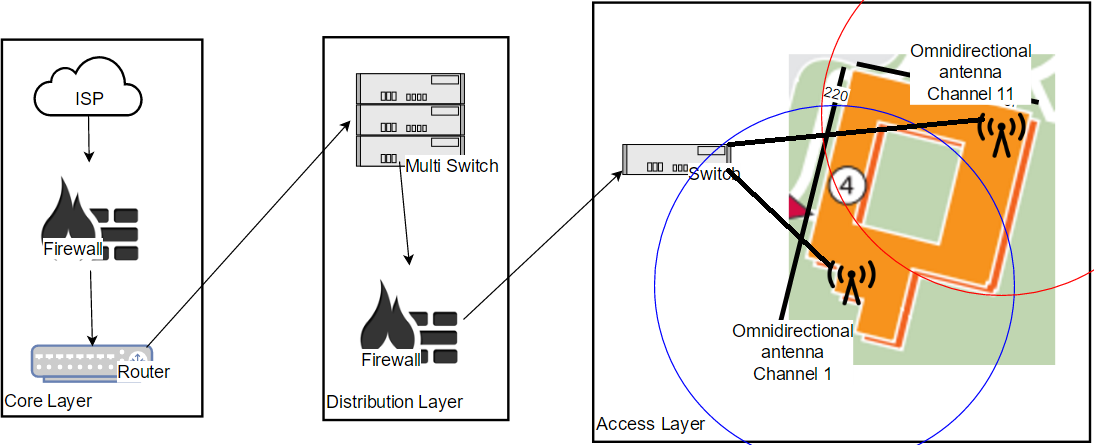
Right

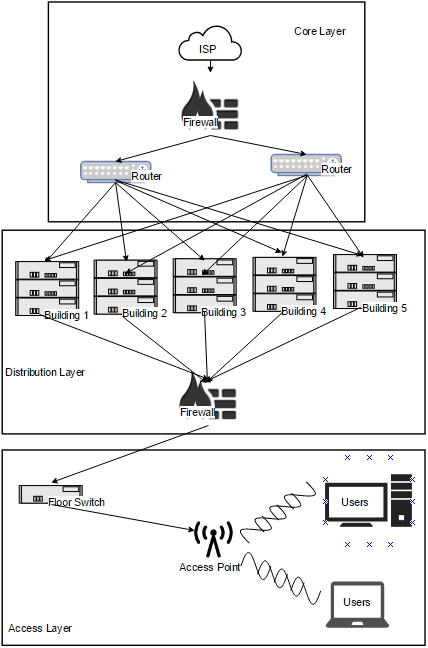


|  |  |  |  |
| --- | --- | --- | --- |
|  | Building name | Floor (ground floor = 1 and 1st floor = 2) | Number of access point |
| 1 | Alexander Jones Building (AJB) | 2 | 2 |
| 2 | Angela Hall | 4 | 4 |
| 3 | Austin Hall | 4 | 4 |
| 4 | Business School (LHBS | 2 | 4 |
| 5 | Chapel (Hope Park) | 1 | 2 |
| 6 | Chaplaincy | 1 | 1 |
| 7 | Conference Centre | 1 | 1 |
| 8 | EDEN (Education and Enterprise) Building) (This also contains building A,B) | 2 | 10 |
| 9 | Estates | 1 | 1 |
| 10 | Frances Mary Lescher Building (FML) (also contains building C) | 4 | 8 |
| 11 | Fresh Hope Food Court | 1 | 2 |
| 12 | Gateway Building, The | 3 | 6 |
| 13 | Green Lane Annexe (GLA) | 2 | 2 |
| 14 | Green Lane Building (GLB) | 2 | 2 |
| 15 | Hilda Constance Allen Building (HCA) | 3 | 6 |
| 16 | Lecture Theatre Complex (LTC) | 1 | 2 |
| 17 | Main Lodge | 1 | 1 |
| 18 | Markland, The | 2 | 2 |
| 19 | Newman Hall | 4 | 8 |
| 20 | Quad (Sheppard-Worlock Library, The) | 3 | 0 |
| 21 | Senate Room (and Trinity Chapel) | 1 | 1 |
| 22 | Sheppard-Worlock Library, The (SWL) | 2 | 4 |
| 23 | New Sports Complex | 1 | 3 |
| 24 | St Agnes Hall | 3 | 3 |
| 25 | St Elphin Hall | 3 | 3 |
| 26 | St Etheldreda Hall | 3 | 3 |
| 27 | St Margaret Hall | 3 | 3 |
| 28 | New Health Science Building | 1 | 1 |
| 29 | Stand Park Lodge | 2 | 1 |
| 30 | Teresa Hall | 4 | 8 |
| 31 | Taggart Lodge | 2 | 2 |
| 32 | Wesley Hall | 4 | 8 |
|  |  | Total | 108 |

Task 3

This is my physical network diagram. I have the height and width of the building that has been turned into pt. I am using the same scale that I used in my task one which is 1m = 5pt. I have added 2 type of access point that is omnidirectional antennas where that signal is all around and a directional is where the signal is only in the front facing, this is great for avoiding carparks and unwanted collisions between channels. 





logical network diagram of my network. What I have is ISP that has been connected to the firewall to monitor and control threats from outside. From firewall I have the router to forward the data that is being pass, Then I have the multi switch for each buildings and then a Firewall/Authentication server for each buildings so it monitors what the users send to the network. Here its connected to the floor switch, after that I have them to the access point where the user can get their wireless. The reason I have switches for building and floor. Because it’s easy to control and find issue, also if the building switch has an issue it will not affect others. Why I have to 2 rooter is so when one is down the other one will be enough to keep it the internet going.

Task 4

War driving/ parking lot attack is when a person from their packed car uses their device to scan for network using Wide-area Network Interface Coprocessor or Service set identifier to find a poorly protected network. Then capturing data frames that is being transmitted from the Wireless access point. The attacker Over time is able to gather the network name, signal strength and etc. With enough information attacker can download malware to the network, get the company data.

Spoofing is another attack that can happen to the wireless network. This attack is when an attacker impersonates as a user of network to attack. There are different types of ways that a spoofing can occur: -

IP spoofing is when the attackers send IP packets from a false source to hide itself, this causes Denial of service as its overloaded with packets to temporary bring down the network. Also if the attacker is knowledgeable they can “impersonate machines with access permissions and bypass trust-based network security measures.”[VERACODE]

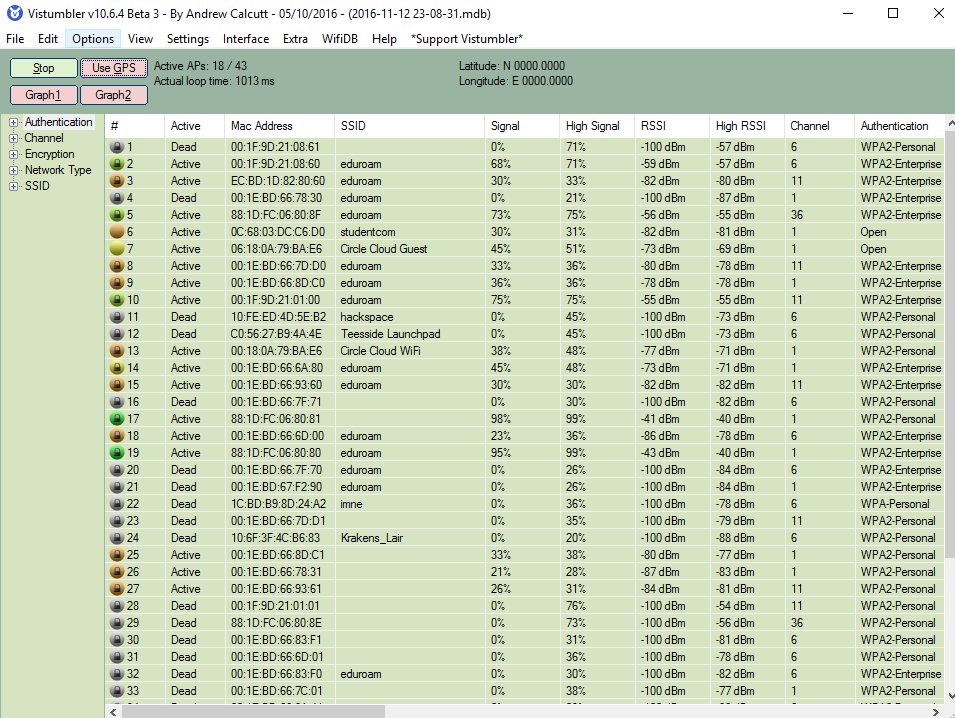
DNS server Spoofing Attacks is another type of spoofing attack. In this attack the attacker redirects domain name to different IP address. The new IP address is for a server that is strictly controlled by the attackers, where the file can be used to spread malware. This all happens when attacker modifies the DNS server.

Packet sniffing is when an attacker intercepts and logging traffic of a network using sniffing software like Wireshark. With the right tools/software the attacker can read the conversation happing between devices in that channel. This can allow such as passwords and other authentication to be capture.

WPS attack is done by using Kali Linux to get the pass word of a wireless network. This is a simple attack that require some knowledge on how to use Linux, if not there are many article that tell you how to do it. With the correct software, good signal and MAC address of the wireless. You enter the detail with the correct code you can get the password. This process is called pixie dust.

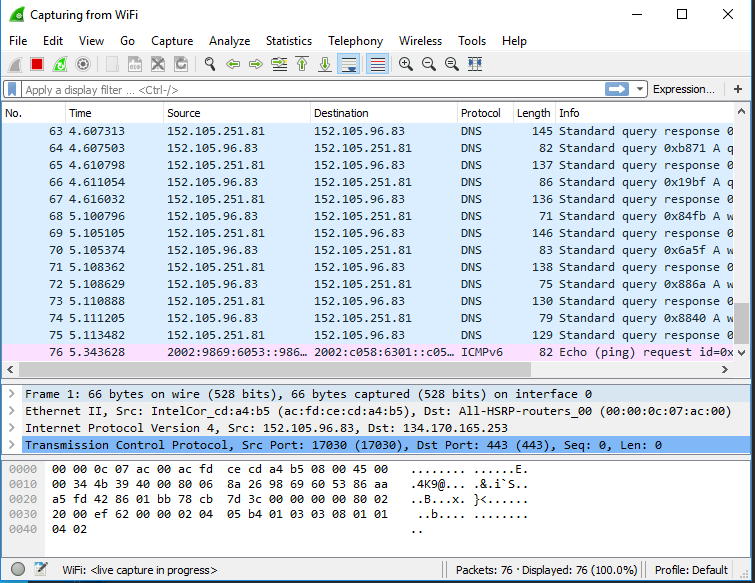
Brute Force is the simplest attack. This is where the attackers try all the passwords one by one till they get the pass word. It doesn’t require any knowledge of programming or any other software. This is basically a try and error. It is not efficiency but they there is no way to prevent it.

Vistumbler



This is one of the software that shows the wireless information. It really easy to use with a press of a button you can get the Mac address, Type of encryptions, if they have authentications, channel and a lot of their information that can be useful to a hacker get what they need. I didn’t have a GPS system device when I was using this but I had used I think there would a lot more information such as the network name, signal strength and RSSI along with their security lever.

Wireshark



Wireshark is used to analyze packets. It captures network packets and its shows that packets data with its details such as where its coming from and where it’s going. What protocol its using. What size the packet and the information and information about the pack like its type and if it requests or not along with if it standard or echo and so on.

Task 5

There is not perfect wireless security against attackers. However, there are a few things I have on my network to make the attackers job harder and my network secure.

I will also have WPA This are protocol. WPA handles the encryptions and decryption keys by changing the key that the system uses. Along with authorizing users by methods of verifying computer’s identity.

WAP2 also another protocol. It uses a process call TKIP to create password with network SSID and passphrase to generate a unique encryption key for wireless network.

Another protocol is CCMP that creates temporary 128-bit keys and 48-bit initialization vector.

A good way to by encrypting and we already have a few but there is a really good encrypting and decrypting tool called ASE encryption algorithm. You have a choice of 128, 192 or 256-bit key. This can be used when sending a secure email.

RADIUS is another protocol but this is a server/client protocol. It has a central server to authenticate the user and their request by remote server. It is a great security as it is a great way for the company to apply policy and for users to follow that policy.

Wireless LAN controller is another security measurement that manages the access point. So if there is a collision or one of the access point is down you have counter measurement so the internet is always up.

Network name or SSID (Service set Identifier) is very essential for an attacker. I will counter this by hiding you SSID.

Just like SSID a lot of attacker attack by using MAC address. To avoid this device will have MAC address filtering. This will define the list of devices and only allow this device on my network.

DDOS attack on a network are possibly the most they of attack that an attacker can do as it is really easy to do. How my network will counter is by black hole filtering. How this work is by placing everything that is undesirable packets to a protected network.

I Have firewall on 2 different lever, one between the ISP and one for each building so it can manage both incoming and outgoing data.

Some of My access points are going to be directional instead of omnidirectional this is to avoid collision but mainly to avoid my channels from reaching the car park where war driving/ parking lot attack is possible.

Task 6

|  |  |  |  |
| --- | --- | --- | --- |
| Name & link | Amount | Price | Total Price |
| Switch  <https://www.comms-express.com/products/netgear-gs748t//?keyword=_cat%3Aswitches%2Fsfps&campaign=332060357&ad=23119224557&ADtype=&Productcode=&gclid=CKLlhOmEstACFaEK0wodEx0FBw> | 105 | £214.49 | £22521.45 |
| Wireless access point  <https://www.amazon.co.uk/gp/product/B013HCO332/ref=zg_bs_430580031_29?ie=UTF8&psc=1&refRID=QJR8J29VR4TJMBG51YTB> | 108 | £34.98 | £3,778.91 |
| Cat6 Cable  <http://www.cablemonkey.co.uk/cat6-rj45-patch-leads/9588-external-cat6-utp-ldpe-rj45-patch-leads.html?ipa=2908&gclid=CKWB8bm9rtACFcyRGwodTk4Erg#/81-length-75m> | 191 | £42.50 | £8,117.50 |
| Antenna  <http://www.myxlshop.co.uk/external-wifi-antenna.html?id=50337454&gclid=CPiAoJe-rtACFc8K0wodp0YHbw> | 321 | £4.39 | £1,409.19 |
| Wireless LAN controller  <https://cableanddevices.co.uk/cisco-2504-wireless-controller-network-management-device.html?gclid=COi0sYCDstACFe0K0wodNRYADA> | 1 | £457.98 | £457.98 |
| Router  <http://www.athema.co.uk/cisco-cisco-2901-terminal-server-bundle-router-desktop-cisco2901-16tsk9-tc01-p-1059921.html?gclid=CK__yZDArtACFbEy0wod6P4Cww> | 2 | £1039.20 | £2,078.40 |
| Firewall  <http://transparent-uk.com/cisco-asa-5505-1u-150mbit-s.html?utm_source=google_shopping&gclid=CJuUqpL4stACFUW4Gwod7nYGUg> | 74 | £398.16 | £13,139.28 |
|  |  | TOTAL | £51,502.71 |

Alternative

Not much has change but it’s just that instead of using firewall for each building have one for each floor. This is so that the process can of management can happen before it gets to switches of floor instead of mine original. This will increase the price but have the same affect so I will be using my original. Also the multiswitch can be for each are instead for each building, how I am going to divide this is by splitting into 4 section so all top left will have its each own section. This will be a lot cheaper but a lot harder to manage the network.

|  |  |  |  |
| --- | --- | --- | --- |
| Name & link | Amount | Price | Total Price |
| Switch  <https://www.comms-express.com/products/netgear-gs748t//?keyword=_cat%3Aswitches%2Fsfps&campaign=332060357&ad=23119224557&ADtype=&Productcode=&gclid=CKLlhOmEstACFaEK0wodEx0FBw> | 77 | £214.49 | £16,746.73 |
| Wireless access point  <https://www.amazon.co.uk/gp/product/B013HCO332/ref=zg_bs_430580031_29?ie=UTF8&psc=1&refRID=QJR8J29VR4TJMBG51YTB> | 108 | £34.98 | £3,778.91 |
| Cat6 Cable  <http://www.cablemonkey.co.uk/cat6-rj45-patch-leads/9588-external-cat6-utp-ldpe-rj45-patch-leads.html?ipa=2908&gclid=CKWB8bm9rtACFcyRGwodTk4Erg#/81-length-75m> | 191 | £42.50 | £8,117.50 |
| Antenna  <http://www.myxlshop.co.uk/external-wifi-antenna.html?id=50337454&gclid=CPiAoJe-rtACFc8K0wodp0YHbw> | 321 | £4.39 | £1,409.19 |
| Wireless LAN controller  <https://cableanddevices.co.uk/cisco-2504-wireless-controller-network-management-device.html?gclid=COi0sYCDstACFe0K0wodNRYADA> | 1 | £457.98 | £457.98 |
| Router  <http://www.athema.co.uk/cisco-cisco-2901-terminal-server-bundle-router-desktop-cisco2901-16tsk9-tc01-p-1059921.html?gclid=CK__yZDArtACFbEy0wod6P4Cww> | 2 | £1039.20 | £2,078.40 |
| Firewall  <http://transparent-uk.com/cisco-asa-5505-1u-150mbit-s.html?utm_source=google_shopping&gclid=CJuUqpL4stACFUW4Gwod7nYGUg> | 74 | £398.16 | £29,463.84 |
|  |  | TOTAL | £62,052.55 |

Task 7

References

DuPaul, N. (2016). *Spoofing Attack: IP, DNS & ARP | Veracode*. [online] Veracode. Available at: https://www.veracode.com/security/spoofing-attack [Accessed 3 Nov. 2016].

ExamCollection. (2016). *Wireless Attacks and Their Types*. [online] Available at: http://www.examcollection.com/certification-training/security-plus-wireless-attacks-and-their-types.html [Accessed 5 Nov. 2016].

Lifewire. (2016). *What Is a Packet Sniffer? - Network Traffic Protocols*. [online] Available at: https://www.lifewire.com/what-is-a-packet-sniffer-2487312 [Accessed 5 Nov. 2016].

SearchITChannel. (2016). *Securing wireless access points: War driving and war walking*. [online] Available at: http://searchitchannel.techtarget.com/feature/Securing-wireless-access-points-War-driving-and-war-walking [Accessed 3 Nov. 2016].

SearchSecurity. (2016). *What is CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol)? - Definition from WhatIs.com*. [online] Available at: http://searchsecurity.techtarget.com/definition/CCMP-Counter-Mode-with-Cipher-Block-Chaining-Message-Authentication-Code-Protocol [Accessed 13 Nov. 2016].

Techterms.com. (2016). *WPA (Wi-Fi Protected Access) Definition*. [online] Available at: http://techterms.com/definition/wpa [Accessed 13 Nov. 2016].

Thesecurityadvocate.com. (2016). *What is ‘Wardriving’ and How Can It Affect Your Company’s Computer Network? | The Security Advocate*. [online] Available at: http://www.thesecurityadvocate.com/2013/03/25/what-is-wardriving-and-how-can-it-affect-your-companys-computer-network/ [Accessed 3 Nov. 2016].

Vistumbler.net. (2016). *Vistumbler - Open Source WiFi scanner and channel scanner for windows*. [online] Available at: https://www.vistumbler.net/ [Accessed 12 Nov. 2016].

Webopedia.com. (2016). *What is WPA2-PSK? Webopedia Definition*. [online] Available at: http://www.webopedia.com/TERM/W/WPA2\_PSK.html [Accessed 13 Nov. 2016].

Wireshark.org. (2016). *Wireshark · Go Deep.*. [online] Available at: https://www.wireshark.org [Accessed 12 Nov. 2016].

WonderHowTo. (2016). *How to Hack WiFi Using a WPS Pixie Dust Attack*. [online] Available at: http://null-byte.wonderhowto.com/how-to/hack-wifi-using-wps-pixie-dust-attack-0162671/ [Accessed 5 Nov. 2016].

Aesencryption.net. (2016). *AES encryption*. [online] Available at: http://aesencryption.net/ [Accessed 17 Nov. 2016].

SearchSecurity. (2016). *What is RADIUS (Remote Authentication Dial-In User Service)? - Definition from WhatIs.com*. [online] Available at: http://searchsecurity.techtarget.com/definition/RADIUS [Accessed 17 Nov. 2016].

Anon, (2016). [online] Available at: http://www.cisco.com/c/dam/en\_us/about/security/intelligence/blackhole.pdf [Accessed 18 Nov. 2016].

En.wikipedia.org. (2016). *Wireless LAN controller*. [online] Available at: https://en.wikipedia.org/wiki/Wireless\_LAN\_controller [Accessed 18 Nov. 2016].

fixedByVonnie. (2016). *3 reasons why hiding your wireless SSID is a bad idea - fixedByVonnie*. [online] Available at: http://www.fixedbyvonnie.com/2014/08/3-reasons-why-hiding-wireless-ssid-bad-idea/#.WC7Q4uaLTcs [Accessed 18 Nov. 2016].

Howtogeek.com. (2016). *Why You Shouldn’t Use MAC Address Filtering On Your Wi-Fi Router*. [online] Available at: http://www.howtogeek.com/204458/why-you-shouldn%E2%80%99t-use-mac-address-filtering-on-your-wi-fi-router/ [Accessed 18 Nov. 2016].

