Report

Campus Plan - Part 1

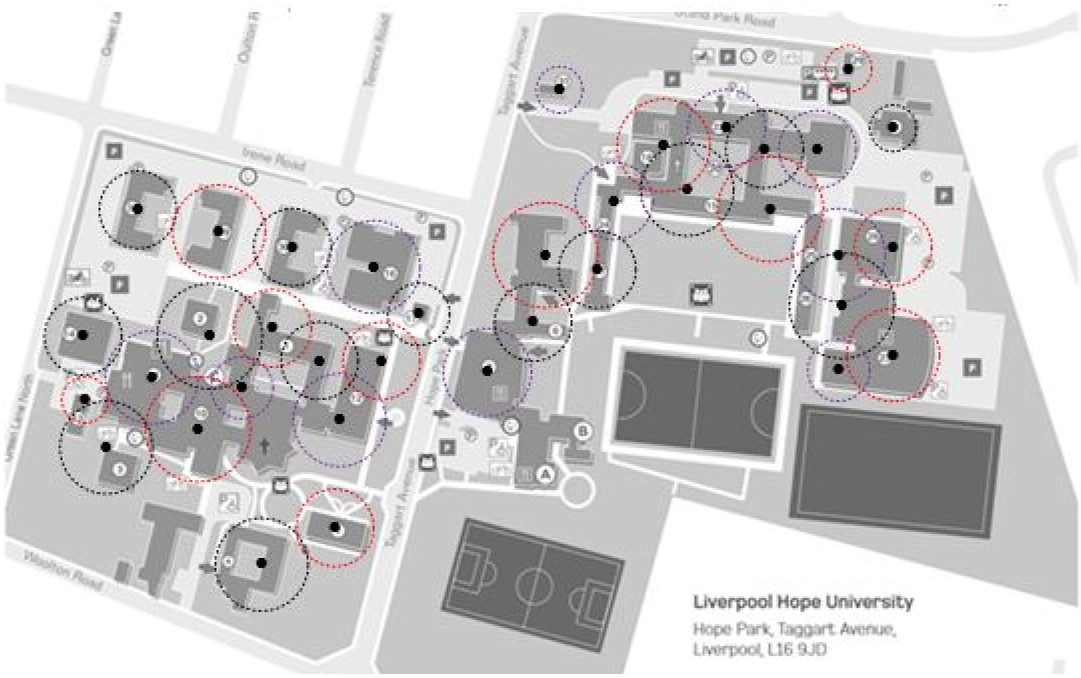
The table below will show the named buildings, floors and measurements of them named buildings, the table will be used on how and where to put wireless access points within the site and make it secure and safe for the university.

Building Number	Building Name	Floors	Measurements
1	Alexander Jones Building (AJB)	1	49m x 59m
2	Angela Hall	4	20m x 20m
3	Austin Hall	4	18m x 18m
4	Business School (LHBS)	1,2	46m x 36m
6	Chaplaincy	2	47m x 68m
7	Conference Centre	1	28m x 33m
8	EDEN (Education and Enterprise) Building	2	46m x 38m
9	Estates	2	17m x 26m
10	Frances Mary Lescher Building (FML)	4	58 m x 34m
11	Fresh Hope Food Court	1	54m x 45m
12	Gateway Building, The	3	82m x 15m
13	Green Lane Annexe (GLA)	2	22m x 9m
14	Green Lane Building (GLB)	2	26m x 26m
15	Hilda Constance Allen Building	3	21m x 63m

	(HCA)		
16	Lecture Theatre Complex (LTC)	1,2	45m x 35m
17	Main Lodge	1	10m x 9m
18	Markland, The	2	18m x 15m
19	Newman Hall	4	43m x 23m
20	Quad (Sheppard-Worlock Library, The)	1	30m x 30m
22	Sheppard-Worlock Library, The (SWL)	2	117m x 28m
23	Hope Park Sports	1	38m x 58m
24/27	St Agnes Hall/St Margaret Hall	3	66m x 8m
25/26	St Elphin Hall/St Etheldreda Hall	3	67m x 10m
28	Health Sciences Building	2	38m x 32m
29	Stand Park Lodge	2	9m x 9m
30	Teresa Hall	4	43m x 22m
31	Taggart Lodge	2	7m x 17m
32	Wesley Hall	4	43m x 23m

Part 2

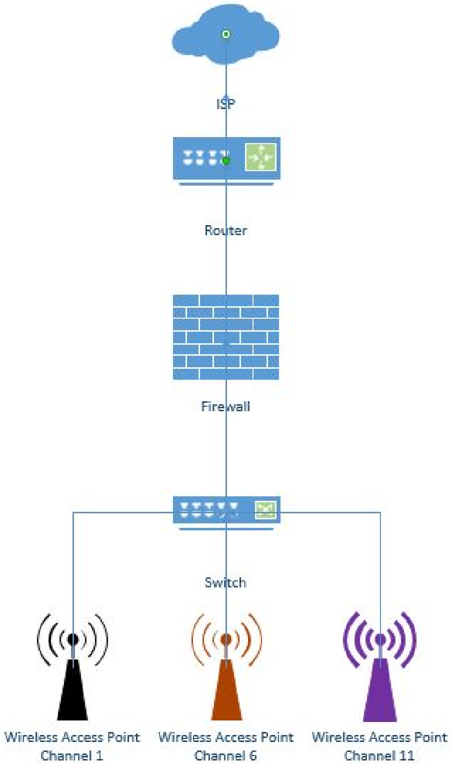
Design off the campus with the location of my wireless access points, it will include all 32 buildings
Key =black access point (Channel 1)/ Red access point (Channel 6)/ Purple access point(Channel 11)



The site map for the hardware to be located are shown above, There are 3 channel I have chosen and made sure the signals of the same channels don't overlap and corrupt or slow down the data on that channel, as shown above the signal strengths are different in distance some are bigger for more surface coverage and others are smaller to reach the smaller buildings or isolated areas of a building. I have used 37 access points on the ground level and will be more depending on the amount of floors the building has. The reason why they are all different signal strength is to prevent packet sniffing. I have added 2, 3 or 4 times more access points on the building that's have more floors as they need the signal to, so the building in the table above with more than 1 floor will have more wireless access points, so the total of the full site is about 75+ access points, i came up with this number as the floors more more access points than a one story building.

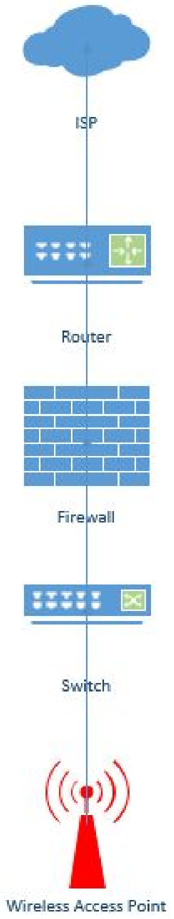
Part 3

The access points i will be using on the site are AIR-CAP2702E-C-K9 Cisco Aironet 2700 Series wireless Access Point(http://www.router-switch.com/air-cap2702e-c-k9-p-5672.html), each have a price of £472 from dollars and i want 75 of them the total number of this will be £35,400. The standard protocols of this AP is 802.11 a/g/n/ac. It runs a signal at 2.4ghz and 5ghz, it is a dual-band also has external antennas for better coverage, also has its own control base which is a big plus so the admins can control the power outage and signal strength benefiting the building and the internet users, but the biggest reason is that it is made by cisco which is a very popular and trusted company which must IT specialist know things about cisco equipment or a lot about them, with a lot of information about the equipment and will be able to remedy the issue if any arrives.


ISP
Router
Firewall
Switch
Wireless Access Point Channel 1
Wireless Access Point Channel 6
Wireless Access Point Channel 11

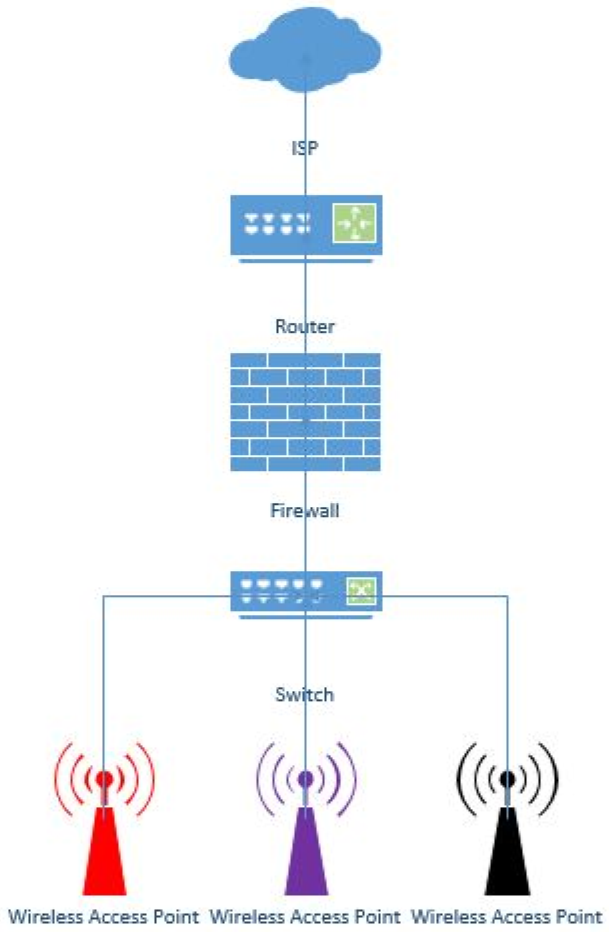
Building 23(Hope Park Sports), The image shown above.

It has three wireless access points, then that goes to a switch which will then go through the firewall stopping any viruses and unwanted data reaching the network, it then goes to a router which will be connected to the network and hard wired computers within the network.



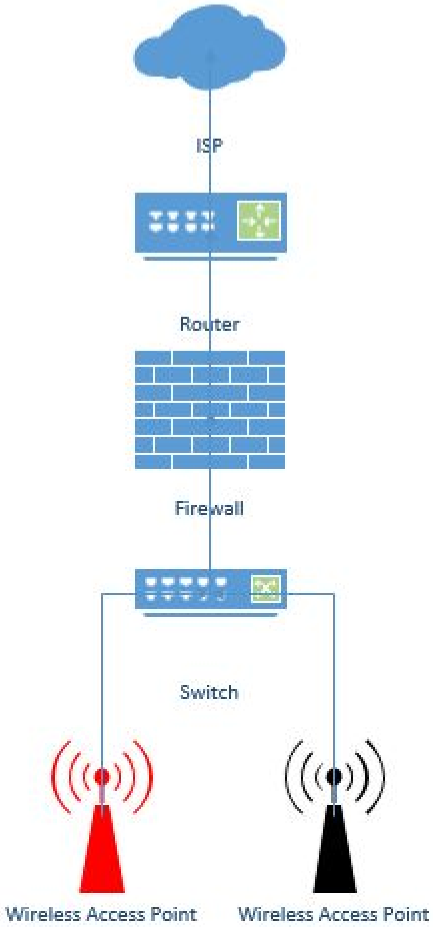
Building 29 (Stand Park Lodge), 2 floors, is the image shown above.

This is easy to setup and use as it will only have 1 access point but 2 floors as the building looks well built the signal will reach though both floors, the channel used is channel 6, The access point will ask the end user to log on before connecting like every other building, it will then go through a switch, then through a firewall to stop unwanted data, viruses etc getting to the network , then goes to a router with other ethernet users then off the the network.



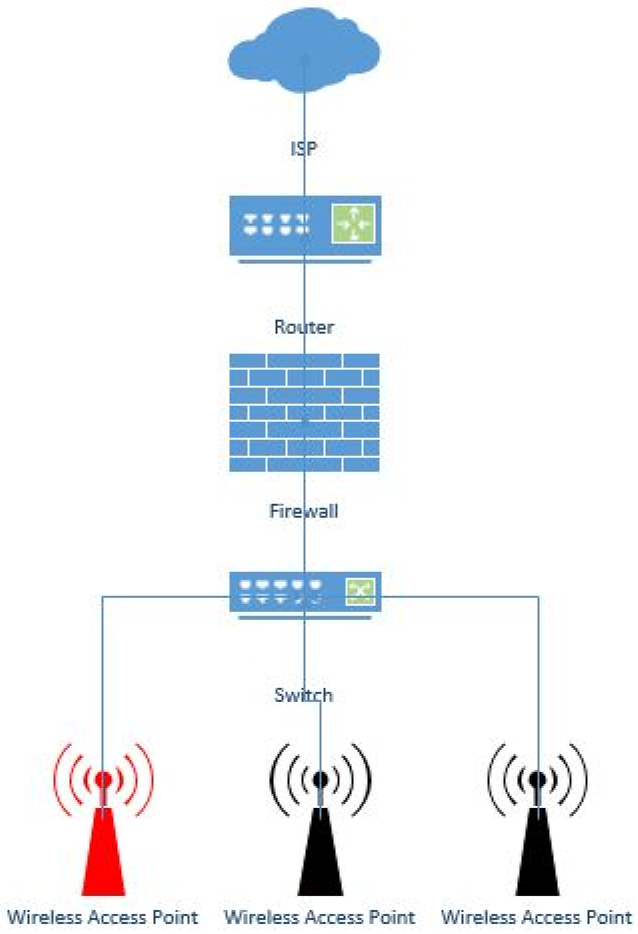
Building 28 (Health Sciences Building), 2 floors, the image shown above.

Their is three access points channel 6 and 11 but channel 1 is from building 22. Again the end user will go through the access points, to a switch then through the firewall, then to the router and off the the network it goes the same way back to the user.



Building 13 (Green Lane Annexe (GLA)), 2 floors. The image above is the design of the access point.

The two access points used are using channel 1 and 6. The channel 1 is from building 3, it is sharing its coverage from building 13. The connection goes through the WAP to the switch, then through the firewall for protection, then to the router with other hardwired computers, then to the network.



Building 6 (Chaplaincy), 2 floors. Is the image shown about the WAP design.

It is using 3 access points 2 channel 1's and 1 channel 6. One of the channel 1's are covered by building 27. Agin the end user will login in to the university site with username and password, and get access, the data will go through the switch, then firewall to stop unwanted data etc getting through then the to router where the other users are connected to then of to the network.

Other installations on the access points, i haven't used any as in i need to buy more equipment for the AP, the only things i have used on the AP is the power it is consuming, the higher the power the more range the signal can get, so the less power less signal it will have. That is the only things i have done to modify the AP signals, the more hardware used the higher the risk on packing sniffing and other attacks could be parent, it will also cost the uni more money, training and they might have more thing go wrong with them, like failing,, crashing and data corruption. The pros of wireless amplifiers or range extenders is that it is hard to control the range it will go as if it goes over the university property, it can breach security risks to its students, data and staff. The main cons of them is that you don’t have to buy as many of that type of hardware and can save money and spend else where or stock up on it in case of a failure.

Possible Security Attacks - Part 4

With the design i have created and want to implement, they could be possible security attacks, for example war driving is a very common way of searching for Wi-Fi, by moving around in a car until a connection is in range, it can be used by laptops, smartphones etc.

The reason people use **war driving** to find possible weak security connections, and they can can the connection and collect packets from people using the connection and can get some important information out of doing that. Another possible security attack and possibly the best one to use against my AP design, as the university has many parking lots and some of the connection can reach to the parking spaces.

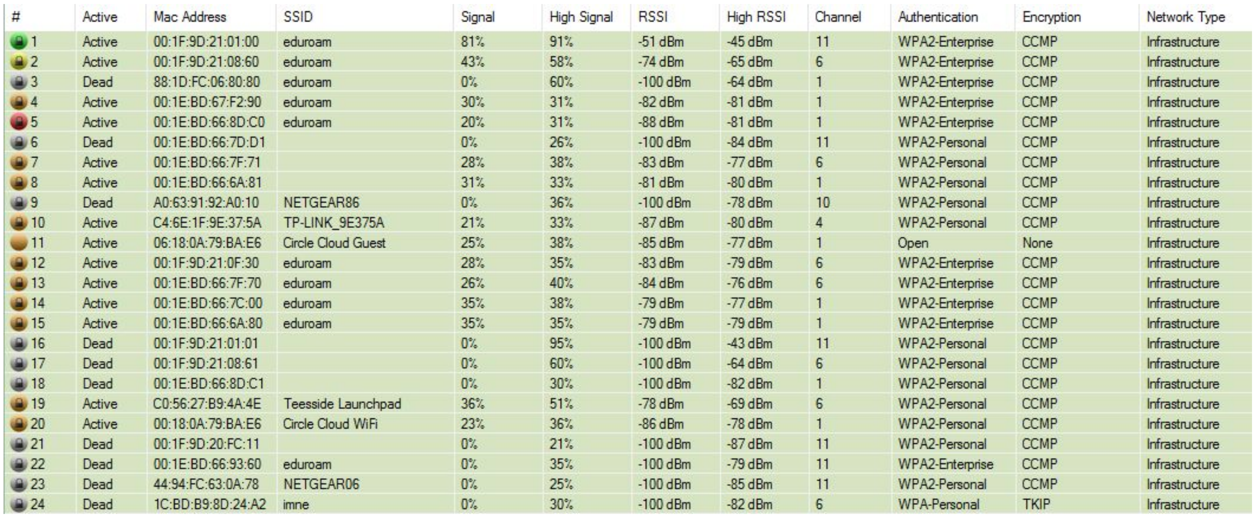
Parking lot attack is the same as war driving but not moving and staying put in the car park and use packet sniffing software like wireshark etc.

DoS (Denial of service) is an attacks where hackers will attempt to prevent the real users from accessing their accounts and services, it is when the attackers send excessive messages to the network of that company asking for the authentication request, because they are sending so many request like in the 100 thousand mark or even more on different devices, it will make the company's service slow and sluggish and even crash and bring down the system for as long as they can.

Then finally spoofing attacks can be done very easy by using a software or a console command prompt, just that the software is setup for doing this type of attacking and you can modify the command prompt, to do a similar thing, but the the university might have a lock on how many time you can send request to the server.

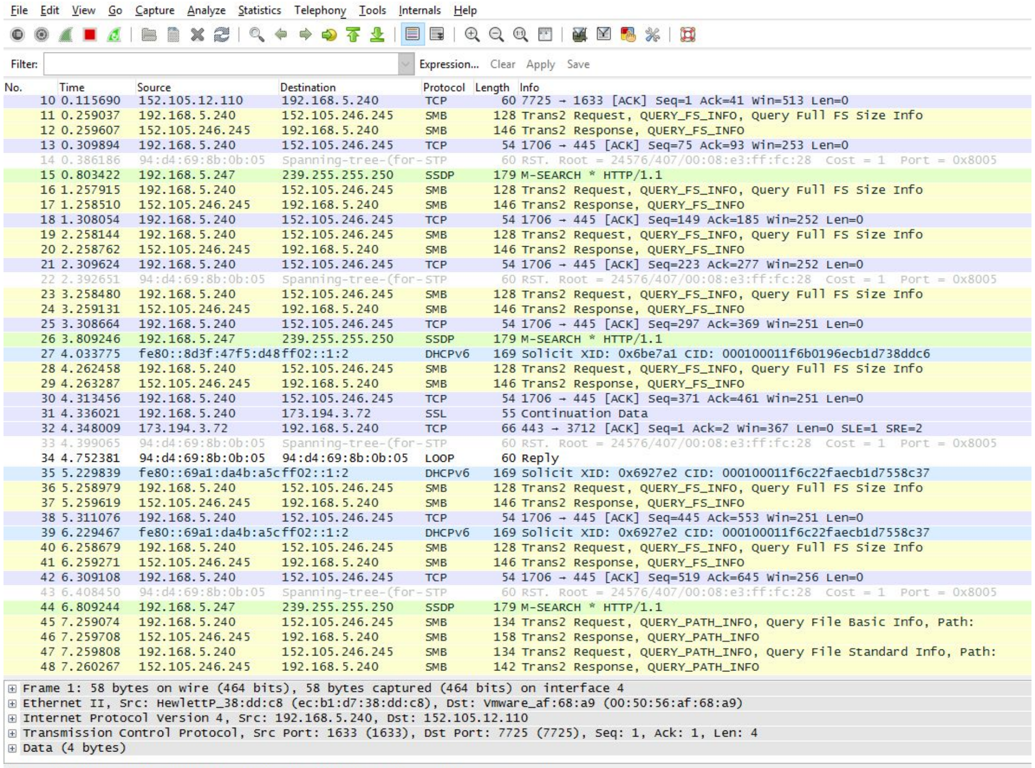
I will be showing 2 software that are programed and can be used to do these attacks.

The first one will be Vistumbler, The image below will show and support how easy it is to packet sniff, it will have the MAC address of the access point, it will have the name of the connection, the signal strength, the channel it is operating on, The authentication it is using like WPA2,WPA and Open, and the encryption type it is using to stop these attacks in some way.



#	Active	Mac Address	SSID	Signal	High Signal	RSSI	High RSSI	Channel	Authentication	Encryption	Network Type
1	Active	00:1F:9D:21:01:00	eduroam	81%	91%	-51 dBm	-45 dBm	11	WPA2-Enterprise	CCMP	Infrastructure
2	Active	00:1F:9D:21:08:60	eduroam	43%	58%	-74 dBm	-65 dBm	6	WPA2-Enterprise	CCMP	Infrastructure
3	Dead	88:1D:FC:06:80:80	eduroam	0%	60%	-100 dBm	-64 dBm	1	WPA2-Enterprise	CCMP	Infrastructure
4	Active	00:1E:BD:67:F2:90	eduroam	30%	31%	-82 dBm	-81 dBm	1	WPA2-Enterprise	CCMP	Infrastructure
5	Active	00:1E:BD:66:8D:C0	eduroam	20%	31%	-88 dBm	-81 dBm	1	WPA2-Enterprise	CCMP	Infrastructure
6	Dead	00:1E:BD:66:7D:D1		0%	26%	-100 dBm	-84 dBm	11	WPA2-Personal	CCMP	Infrastructure
7	Active	00:1E:BD:66:7F:71		28%	38%	-83 dBm	-77 dBm	6	WPA2-Personal	CCMP	Infrastructure
8	Active	00:1E:BD:66:6A:81		31%	33%	-81 dBm	-80 dBm	1	WPA2-Personal	CCMP	Infrastructure
9	Dead	A0:63:91:92:A0:10	NETGEAR86	0%	36%	-100 dBm	-78 dBm	10	WPA2-Personal	CCMP	Infrastructure
10	Active	C4:6E:1F:9E:37:5A	TP-LINK_9E375A	21%	33%	-87 dBm	-80 dBm	4	WPA2-Personal	CCMP	Infrastructure
11	Active	06:18:0A:79:BA:E6	Circle Cloud Guest	25%	38%	-85 dBm	-77 dBm	1	Open	None	Infrastructure
12	Active	00:1F:9D:21:0F:30	eduroam	28%	35%	-83 dBm	-79 dBm	6	WPA2-Enterprise	CCMP	Infrastructure
13	Active	00:1E:BD:66:7F:70	eduroam	26%	40%	-84 dBm	-76 dBm	6	WPA2-Enterprise	CCMP	Infrastructure
14	Active	00:1E:BD:66:7C:00	eduroam	35%	38%	-79 dBm	-77 dBm	1	WPA2-Enterprise	CCMP	Infrastructure
15	Active	00:1E:BD:66:6A:80	eduroam	35%	35%	-79 dBm	-79 dBm	1	WPA2-Enterprise	CCMP	Infrastructure
16	Dead	00:1F:9D:21:01:01		0%	95%	-100 dBm	-43 dBm	11	WPA2-Personal	CCMP	Infrastructure
17	Dead	00:1F:9D:21:08:61		0%	60%	-100 dBm	-64 dBm	6	WPA2-Personal	CCMP	Infrastructure
18	Dead	00:1E:BD:66:8D:C1		0%	30%	-100 dBm	-82 dBm	1	WPA2-Personal	CCMP	Infrastructure
19	Active	C0:56:27:B9:4A:4E	Teesside Launchpad	36%	51%	-78 dBm	-69 dBm	6	WPA2-Personal	CCMP	Infrastructure
20	Active	00:18:0A:79:BA:E6	Circle Cloud WiFi	23%	36%	-86 dBm	-78 dBm	1	WPA2-Personal	CCMP	Infrastructure
21	Dead	00:1F:9D:20:FC:11		0%	21%	-100 dBm	-87 dBm	11	WPA2-Personal	CCMP	Infrastructure
22	Dead	00:1E:BD:66:93:60	eduroam	0%	35%	-100 dBm	-79 dBm	11	WPA2-Enterprise	CCMP	Infrastructure
23	Dead	44:94:FC:63:0A:78	NETGEAR06	0%	25%	-100 dBm	-85 dBm	11	WPA2-Personal	CCMP	Infrastructure
24	Dead	1C:BD:B9:8D:24:A2	imne	0%	30%	-100 dBm	-82 dBm	6	WPA-Personal	TKIP	Infrastructure

The next software is called wireshark, it is also used for these attacks, but both of these are used by administration of the company to monitor the network. The image shown below, shows the source of the request, which is the IP address and sometimes the MAC address, and will show the final destination of the request which is IP and MAC address depending on the hardware used like computers, switches etc. It will show the Protocol it is running off for example TCP, DHCP etc. Then it tells the attacker the info of the request and will be able to pick a signal and use it for their benefit.



```
No.     Time      Source             Destination        Protocol Length Info
     10 0.115690  152.105.12.110     192.168.5.240      TCP        60 7725 → 1633 [ACK] Seq=1 Ack=41 Win=513 Len=0
     11 0.259037  192.168.5.240      152.105.246.245    SMB       128 Trans2 Request, QUERY_FS_INFO, Query Full FS Size Info
     12 0.259607  152.105.246.245    192.168.5.240      SMB       146 Trans2 Response, QUERY_FS_INFO
     13 0.309894  192.168.5.240      152.105.246.245    TCP        54 1706 → 445 [ACK] Seq=75 Ack=93 Win=253 Len=0
     14 0.386186  94:d4:69:8b:0b:05  Spanning-tree-(for-STP        60 RST. Root = 24576/407/00:08:e3:ff:fc:28  Cost = 1  Port = 0x8005
     15 0.803422  192.168.5.247      239.255.255.250    SSDP      179 M-SEARCH * HTTP/1.1
     16 1.257915  192.168.5.240      152.105.246.245    SMB       128 Trans2 Request, QUERY_FS_INFO, Query Full FS Size Info
     17 1.258510  152.105.246.245    192.168.5.240      SMB       146 Trans2 Response, QUERY_FS_INFO
     18 1.308054  192.168.5.240      152.105.246.245    TCP        54 1706 → 445 [ACK] Seq=149 Ack=185 Win=252 Len=0
     19 2.258144  192.168.5.240      152.105.246.245    SMB       128 Trans2 Request, QUERY_FS_INFO, Query Full FS Size Info
     20 2.258762  152.105.246.245    192.168.5.240      SMB       146 Trans2 Response, QUERY_FS_INFO
     21 2.309624  192.168.5.240      152.105.246.245    TCP        54 1706 → 445 [ACK] Seq=223 Ack=277 Win=252 Len=0
     22 2.392651  94:d4:69:8b:0b:05  Spanning-tree-(for-STP        60 RST. Root = 24576/407/00:08:e3:ff:fc:28  Cost = 1  Port = 0x8005
     23 3.258480  192.168.5.240      152.105.246.245    SMB       128 Trans2 Request, QUERY_FS_INFO, Query Full FS Size Info
     24 3.259131  152.105.246.245    192.168.5.240      SMB       146 Trans2 Response, QUERY_FS_INFO
     25 3.308664  192.168.5.240      152.105.246.245    TCP        54 1706 → 445 [ACK] Seq=297 Ack=369 Win=251 Len=0
     26 3.809246  192.168.5.247      239.255.255.250    SSDP      179 M-SEARCH * HTTP/1.1
     27 4.033775  fe80::8d3f:47f5:d48ff02::1:2          DHCPv6    169 Solicit XID: 0x6be7a1 CID: 000100011f6b0196ecb1d738ddc6
     28 4.262458  192.168.5.240      152.105.246.245    SMB       128 Trans2 Request, QUERY_FS_INFO, Query Full FS Size Info
     29 4.263287  152.105.246.245    192.168.5.240      SMB       146 Trans2 Response, QUERY_FS_INFO
     30 4.313456  192.168.5.240      152.105.246.245    TCP        54 1706 → 445 [ACK] Seq=371 Ack=461 Win=251 Len=0
     31 4.336021  192.168.5.240      173.194.3.72       SSL        55 Continuation Data
     32 4.348009  173.194.3.72       192.168.5.240      TCP        66 443 → 3712 [ACK] Seq=1 Ack=2 Win=367 Len=0 SLE=1 SRE=2
     33 4.399065  94:d4:69:8b:0b:05  Spanning-tree-(for-STP        60 RST. Root = 24576/407/00:08:e3:ff:fc:28  Cost = 1  Port = 0x8005
     34 4.752381  94:d4:69:8b:0b:05  94:d4:69:8b:0b:05  LOOP       60 Reply
     35 5.229839  fe80::69a1:da4b:a5cff02::1:2          DHCPv6    169 Solicit XID: 0x6927e2 CID: 000100011f6c22faecb1d7558c37
     36 5.258979  192.168.5.240      152.105.246.245    SMB       128 Trans2 Request, QUERY_FS_INFO, Query Full FS Size Info
     37 5.259619  152.105.246.245    192.168.5.240      SMB       146 Trans2 Response, QUERY_FS_INFO
     38 5.311076  192.168.5.240      152.105.246.245    TCP        54 1706 → 445 [ACK] Seq=445 Ack=553 Win=251 Len=0
     39 6.229467  fe80::69a1:da4b:a5cff02::1:2          DHCPv6    169 Solicit XID: 0x6927e2 CID: 000100011f6c22faecb1d7558c37
     40 6.258679  192.168.5.240      152.105.246.245    SMB       128 Trans2 Request, QUERY_FS_INFO, Query Full FS Size Info
     41 6.259271  152.105.246.245    192.168.5.240      SMB       146 Trans2 Response, QUERY_FS_INFO
     42 6.309108  192.168.5.240      152.105.246.245    TCP        54 1706 → 445 [ACK] Seq=519 Ack=645 Win=256 Len=0
     43 6.408450  94:d4:69:8b:0b:05  Spanning-tree-(for-STP        60 RST. Root = 24576/407/00:08:e3:ff:fc:28  Cost = 1  Port = 0x8005
     44 6.809244  192.168.5.247      239.255.255.250    SSDP      179 M-SEARCH * HTTP/1.1
     45 7.259074  192.168.5.240      152.105.246.245    SMB       134 Trans2 Request, QUERY_PATH_INFO, Query File Basic Info, Path:
     46 7.259708  152.105.246.245    192.168.5.240      SMB       158 Trans2 Response, QUERY_PATH_INFO
     47 7.259808  192.168.5.240      152.105.246.245    SMB       134 Trans2 Request, QUERY_PATH_INFO, Query File Standard Info, Path:
     48 7.260267  152.105.246.245    192.168.5.240      SMB       142 Trans2 Response, QUERY_PATH_INFO
```

```
⊞ Frame 1: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface 4
⊞ Ethernet II, Src: HewlettP_38:dd:c8 (ec:b1:d7:38:dd:c8), Dst: Vmware_af:68:a9 (00:50:56:af:68:a9)
⊞ Internet Protocol Version 4, Src: 192.168.5.240, Dst: 152.105.12.110
⊞ Transmission Control Protocol, Src Port: 1633 (1633), Dst Port: 7725 (7725), Seq: 1, Ack: 1, Len: 4
⊞ Data (4 bytes)
```

So the security risks are high on high earning companies like university's, bank’s etc. So the better the protocol, encryption type and authentication. The harder it will be for these attackers to get the packets, data and information from the university. The sites i have talked about are free to download and easy to use and have a big online following.

Countermeasures against security attacks - Part 5

I will be briefly explaining the countermeasures against the security attacks, then talking about WPA, WPA2, TKIP/ CCMP, AES, RADIUS authentication and VPN.

The countermeasures against security attacks is to have a very good authentication server, Only allow the signal strength to go so far anymore and it could be packet sniffed another one is have the company purchase a larger network space so when attacks do happen the network will be able to handle the DoS attacks.

Firstly **WPA** is short for (Wi-Fi protected access), it was made to improve on the security features of WEP, it is more sophisticated at encrypting data than the older WEP, it will also provide user authentication which is one of the best standards to you for a university network as each end user will need to use there authentication like username and password to access their work spaces.

WPA2 is short for (Wi-Fi protected access 2) is the next security method to WPA, it provides a stronger data protection, the main reason and best to use this one is that it will provide the university and their staff and students. It only lets authorized users to be able to access their wireless network. The security of WPA2 has not been cracked as of now and provides government grade security.

TKIP is short for (Temporal Key Integrity Protocol), it is a encryption protocol that is included in the IEEE 802.11i standard, it was created to be able to provide a lot more encryption security than the older standard WEP, the TKIP is used in the WPA encryption method.

CCMP is short for (Counter mode with cipher block chaining message authentication code protocol), it is a encryption protocol that is formed up into 802.11i, CCMP has better security compared to the other one TKIP, CCMP minimises the vulnerability to replay attacks, but it will requires additional processing power compared to TKIP.

AES is short for (advanced encryption standard), it is a symmetric block cipher and employed by the US government which they use to protect classified information, and it is implemented in hardware and software around the world to encrypt the sensitive data.

RADIUS authentication is short for (remote authentication dial-in user service), it is a client/server protocol and with the software it uses enables the remote access servers to be able to communicate with the main server to authenticate the dial-in users and able to authorize the access to the requested system or service, the RADIUS will allow the university to maintain the user profiles in the central databases. It provides very good security by allowing the company to be able to set up policies.

VPN is short for virtual private network, it is a private network that can be set up by anyone at home or for a company. It keeps the cost down for the company and has very good security, as the admins or network team of a company can monitor more easily.

Cost of Implementing - Part 6

The table below will display, the hardware needed, the number of each hardware needed, total cost of for that hardware and a hyperlink to the website i used to collect this data.

Hardware	No. of	Total Cost	Link
Access Points	75x	£35.400	http://www.router-switch.com/air-cap2702e-c-k9-p-5672.html
Switches	30x	£30.197.40	http://www.ebuyer.com/363240-cisco-small-business-sg500-52-48-port-gigabit-stackable-managed-switch-sg500-52-k9-g5
Antennas	External antennas are included in Access Points		
50m Cables	10x	£220	http://www.cabling4less.co.uk/category.php?cat_id=158

Reference

1. SearchSecurity. 2016. *What is Advanced Encryption Standard (AES)? - Definition from WhatIs.com*. [ONLINE] Available at: http://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard. [Accessed 18 November 2016].
2. 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 18 November 2016].
3. 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 18 November 2016].