



PROPOSAL

Wireless Attack On WPA2 Using Aircrack-ng

OLEH:

MUHAMMAD ABRAR AIMAN BIN SHAH EDIN

MUHAMMAD AFIZ HAKIMI BIN ARIFFIN

PENYELIA PROJEK:

PUAN NURULAFIZA BINTI RAMLI

SESI 2/2022:

DIPLOMA TEKNOLOGI KOMPUTER RANGKAIAN

INSTITUT LATIHAN PERINDUSTRIAN

KUALA LANGAT SELANGOR

ISI KANDUNGAN

NO	ISI KANDUNGAN	MUKA SURAT
1	PENGENALAN PROJEK	3
2	PENYATAAN MASALAH	3
3	OBJEKTIF PROJEK	4
4	FAEDAH PROJEK	4
5	SKOP PROJEK	4
6	REKABENTUK PROJEK	5
7	SENARAI BAHAN DAN ANGGARAN KOS	6-8
8	CARTA GANTT DAN PERANCANGAN PROJEK	9-12
9	KESIMPULAN	13

PENGENALAN PROJEK

Wireless Fidelity (Wi-Fi), telah menjadi satu keperluan dalam kehidupan seharian kita. Lebih satu bilion *access point Wi-Fi* menghubungkan hampir ratus bilion peranti IoT, telefon pintar, tablet, komputer riba, *desktop*, TV pintar, kamera video, *monitor*, pencetak dan peranti pengguna lain ke Internet untuk membolehkan berjuta-juta aplikasi mencapai semua orang, di mana-mana. *Wireless network* seperti *wifi* adalah sangat penting bagi pengguna. Khususnya kepada pengguna yang ingin bergerak 'bebas' dari *ethernet cable* yang sentiasa mengekang mobiliti pengguna. Namun dalam faedah *wireless network*, terdapat juga risiko dan bahaya yang akan terjadi bila sesebuah *wireless* mempunyai sistem keselamatan yang lemah. Atas sebab itu, serangan terhadap *wireless network* juga telah meningkat sejajar dengan perkembangan sistem keselamatan teknologi *wireless* yang pesat.

PENYATAAN MASALAH

Mengekalkan keselamatan rangkaian *wireless* adalah amat penting. Rangkaian *wireless* yang gunakan untuk memindahkan dan menghantar data seperti nama pengguna, kata laluan, butiran kad dan data sensitif lain. Jika rangkaian *wireless* yang gunakan tidak selamat, pengguna berisiko menghadapi kehilangan data peribadi. Permasalahan terjadi apabila adanya kelemahan sistem rangkaian atau perkakasan, sebagai contoh *access point* mudah untuk ditembusi dan dicerobohi. Selain daripada itu juga sikap individu yang tidak bertanggungjawab cuba untuk menggodam rangkaian atau perkakasan demi kepentingan peribadi. Oleh itu, antara salah satu cara untuk mengelakkan *AP* dari diserang adalah dengan menggunakan *mac binding whitelist*.

OBJEKTIF PROJEK

- ❖ Membuat serangan terhadap Access point (AP) dengan menggunakan Aircrack-ng.
- ❖ Membangunkan MAC Binding Whitelist untuk meningkatkan keselamatan WLAN.

FAEDAH PROJEK

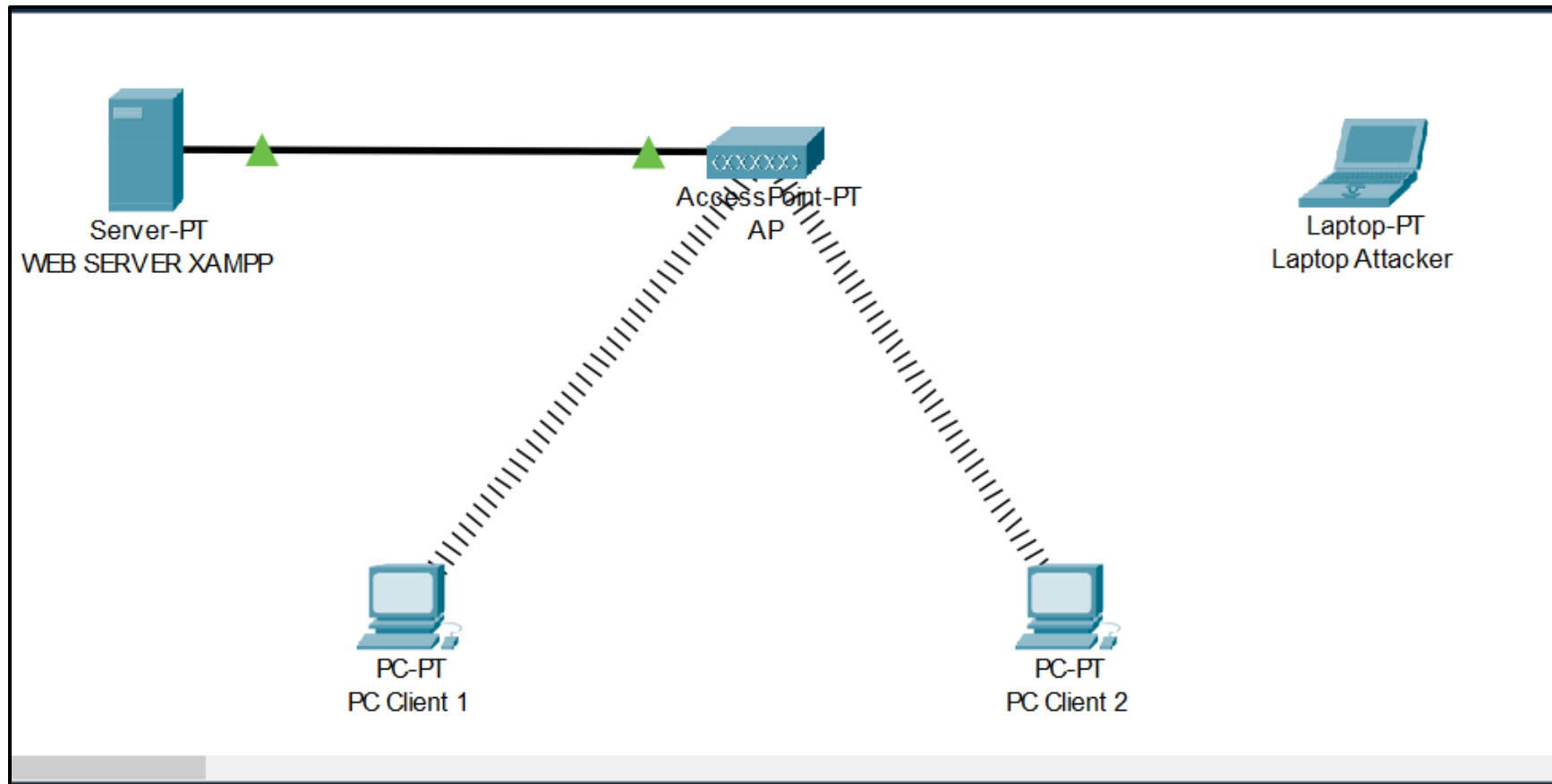
Faedah yang didapati dari penghasilan projek ini adalah keselamatan data peribadi semua pengguna yang menggunakan WLAN akan terjamin. Hal ini kerana adanya penyelesaian masalah yang dibuat bagi mengatasi masalah yang dihadapi.

SKOP PROJEK

Projek ini adalah mengenai teknologi *wireless* yang diserang oleh individu yang tidak dikenali. Skop kajian ditetapkan adalah bertujuan untuk memberikan penekanan kepada hala tuju sebenar kajian ini. Antara skop projek ini adalah:





- 1) Membangunkan *web server* untuk diakses oleh pengguna.
- 2) Membuat serangan dengan menggunakan *software tools aircrack-ng* pada OS *Kali Linux* bagi membuat serangan terhadap AP.
- 3) Membangunkan *MAC Binding Whitelist* secara *manual* pada AP bagi mempertahankan WLAN dari diserang.

REKABENTUK





RAJAH 1 – NETWORK DIAGRAM PROJECT

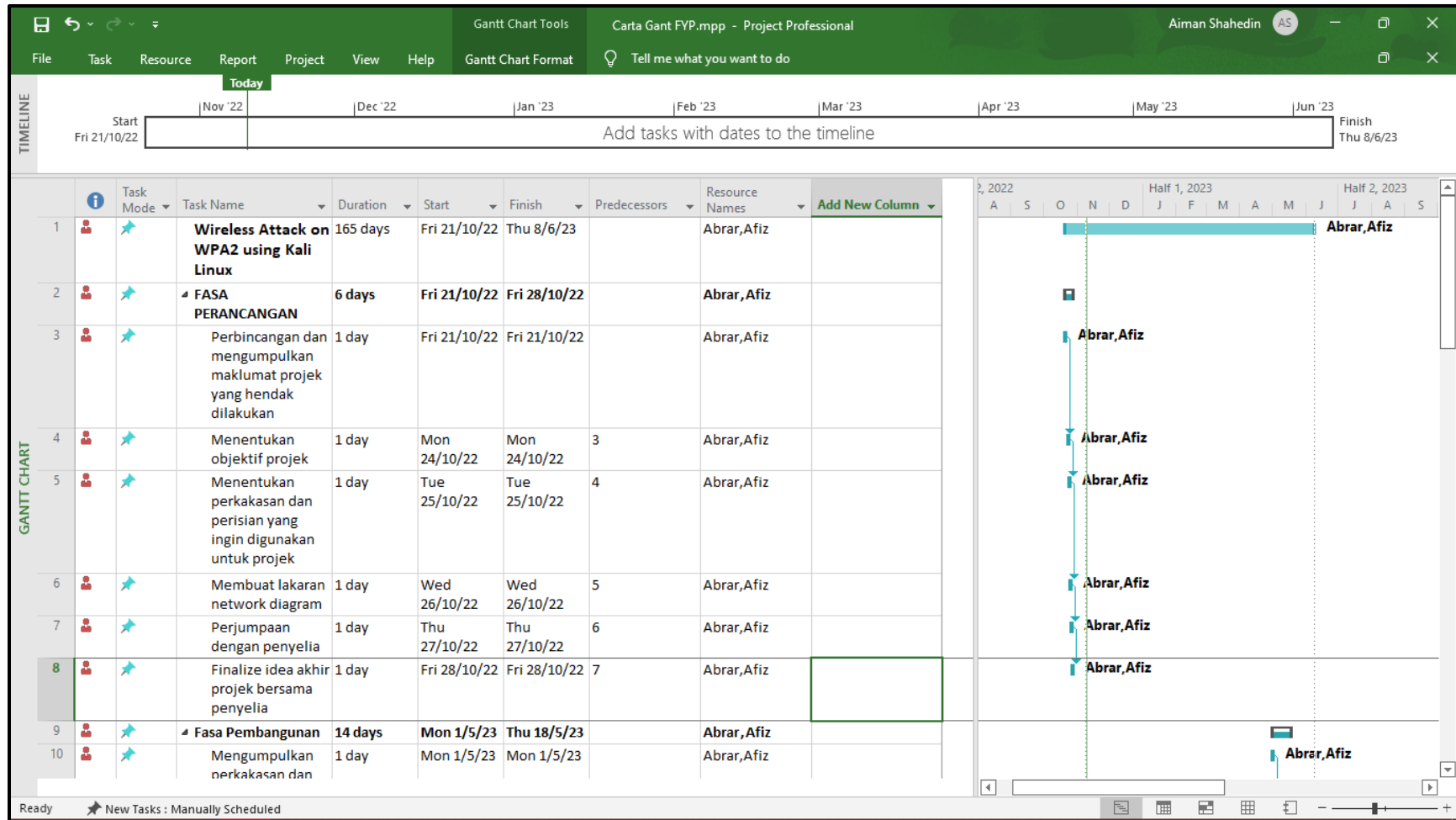
SENARAI BAHAN DAN ANGGARAN KOS

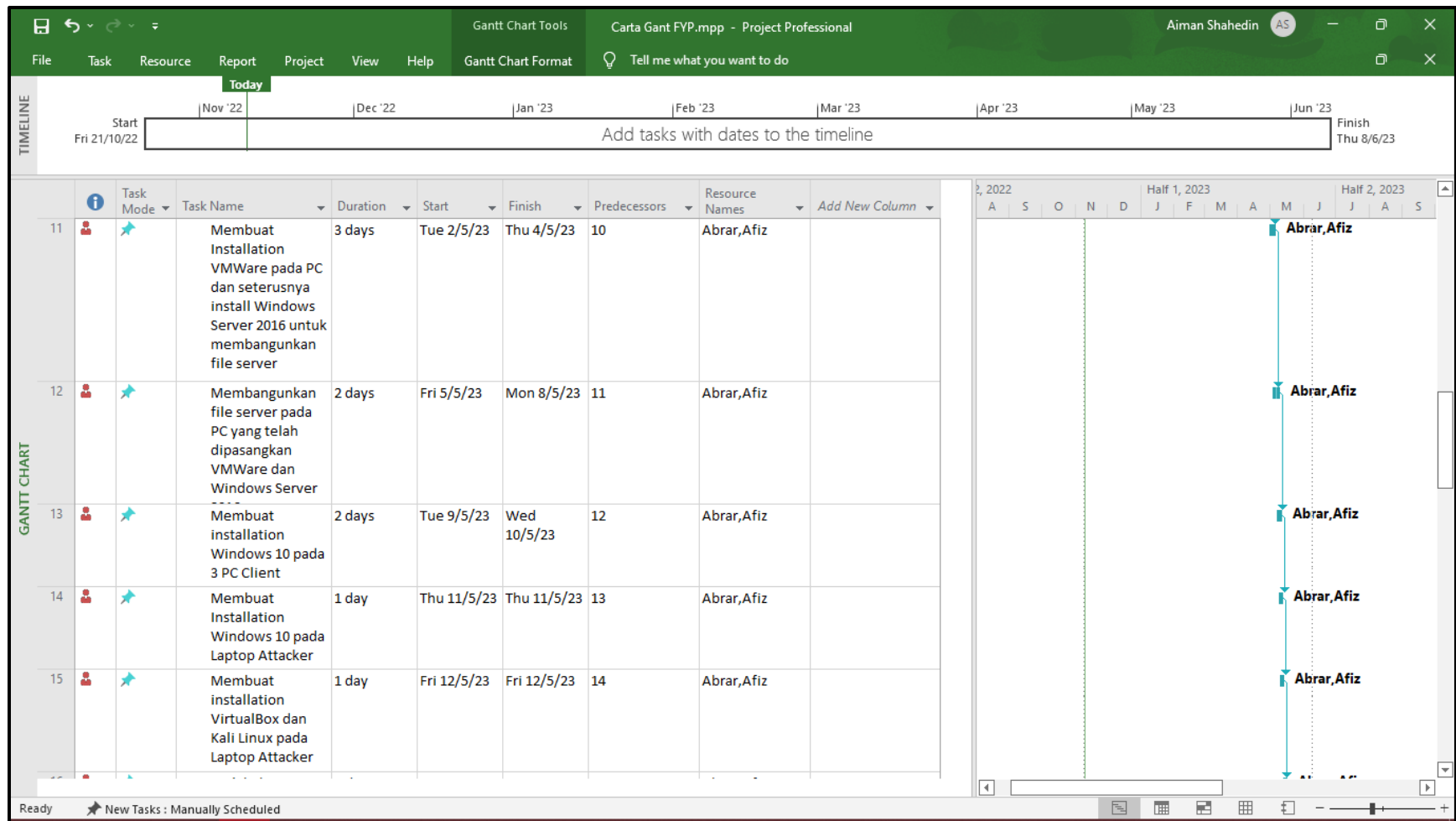
ITEM	NAMA	FUNGSI BARANG	HARGA
 <i>Wifi Adapter</i>	<i>Tp-link wifi adapter</i>	<ul style="list-style-type: none"> Menerima dan berkongsi isyarat wifi ke <i>laptop attacker</i> atau <i>pc client</i> Mengakses sambungan internet berkelajuan tinggi 	RM29.00
 <i>Laptop</i>	<i>Laptop Lenovo Ideapad S145</i>	<ul style="list-style-type: none"> Berfungsi sebagai <i>laptop attacker</i> di dalam projek ini Sebagai <i>device</i> yang digunakan untuk membuat penyerangan terhadap AP 	RM1,499.00
 <i>Access Point</i>	<i>Access Point TP-Link TL-WA801N</i>	<ul style="list-style-type: none"> Sambung ke <i>Ethernet Cable</i> untuk untuk membuat rangkaian <i>wireless</i> serta kongsi WLAN kepada semua peranti <i>wireless</i> 	RM125.99
 <i>Computer</i>	<i>Lenovo m90p computer set</i>	<ul style="list-style-type: none"> Digunakan sebagai <i>PC Client</i> di dalam projek ini bagi mendapat sambungan <i>wireless</i> dan <i>web server</i> 	RM1089.00

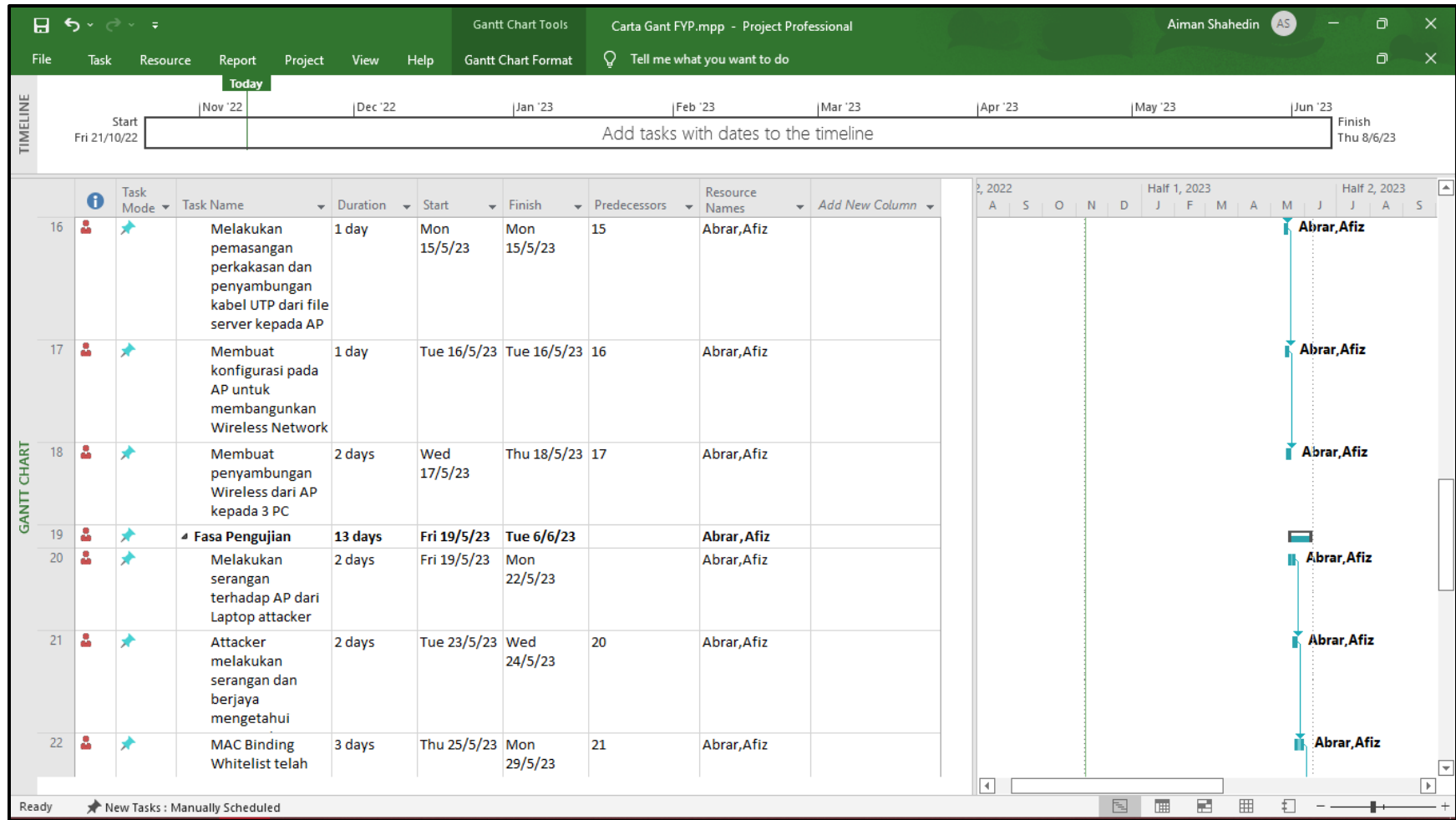
 <p><i>Cable Ethernet Straight utp cat 5</i></p>		<ul style="list-style-type: none"> Berfungsi menyambungkan antara 2 perkakasan rangkaian iaitu web server dan PC Client. 	RM49.00
 <p><i>Linux</i></p>	<i>Kali Linux</i>	<ul style="list-style-type: none"> Berfungsi sebagai OS yang digunakan oleh Laptop Attacker untuk menyerang AP 	Freeware
 <p><i>Windows</i></p>	<i>Windows 10 Professional</i>	<ul style="list-style-type: none"> OS yang digunakan oleh PC Client dan Web Server 	RM550.00
 <p><i>Xampp</i></p>	<i>Xampp</i>	<ul style="list-style-type: none"> Digunakan sebagai platform untuk membangunkan web server di PC Client 	Freeware

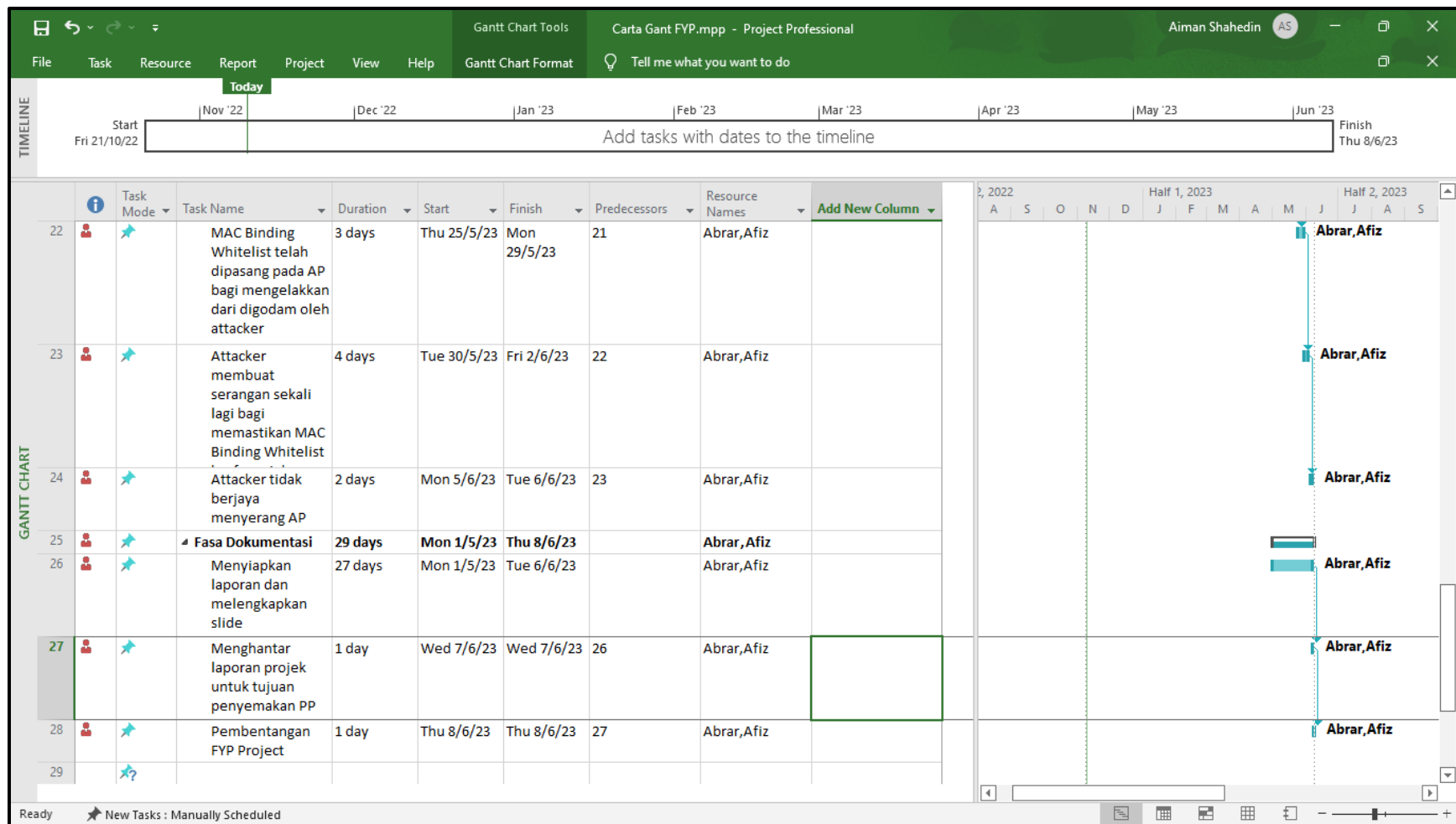
 <p>Virtual Machines</p>	<p>Vmware Workstation</p>	<ul style="list-style-type: none"> Menjadi <i>platform</i> untuk memasang <i>Kali Linux</i> tanpa mengformat semula <i>Winsdows 10</i> pada <i>Laptop Attacker</i> 	<p>Freeware</p>
 <p>Aircrack-ng</p>	<p>Aircrack-ng</p>	<ul style="list-style-type: none"> Digunakan untuk menukar kod fail yang ditangkap <i>airodump-ng</i> kepada kata laluan sebenar di dalam OS <i>Kali Linux</i> pada <i>Laptop Attacker</i> 	<p>Freeware</p>
<p>JUMLAH KOS PERKAKASAN DAN PERISIAN YANG DIGUNAKAN</p>			<p>RM3341.99</p>

CARTA GANTT PERANCANGAN PROJEK









KESIMPULAN

Kesimpulan dari penghasilan projek *Wireless Attack On WPA2 Using Aircrack-ng* ini adalah projek ini sangat penting bagi membuka mata masyarakat bahawa serangan seperti ini wujud di dunia 'nyata'. Oleh disebabkan itu, penghasilan penyelesaian masalah juga telah ditunjukkan di dalam projek ini bertujuan untuk mempertahankan *WLAN* dari diserang.