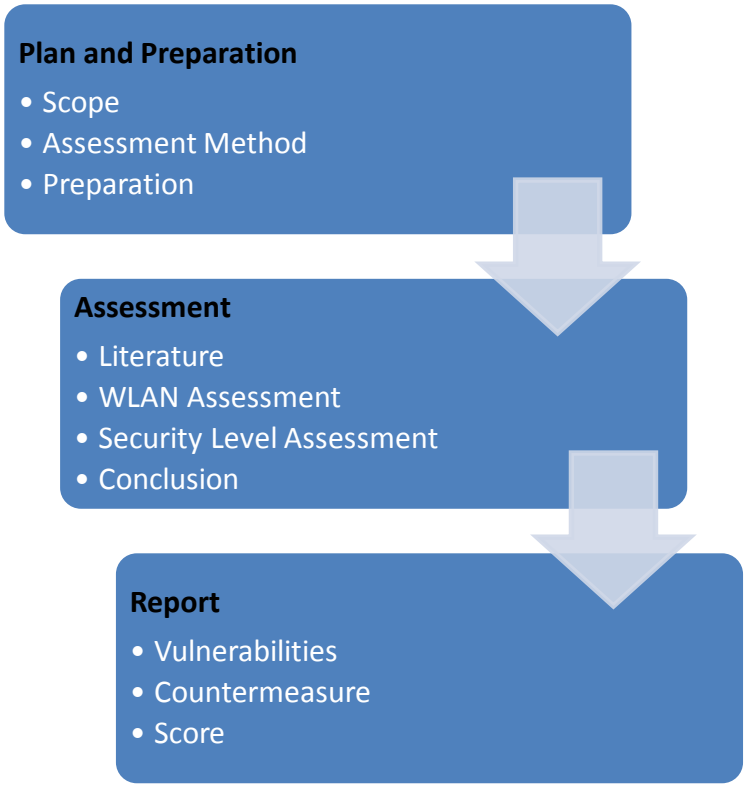
BAB III

METODOLOGI PENELITIAN

3.1. Metodologi Penelitian

Alur pengerjaan penelitian ini adalah seperti pada grafik 3.1. berikut:



Grafik 3.1. Alur Penelitian

3.1.1. *Scope*

Penentuan ruang lingkup penelitian ini ditetapkan berdasarkan jumlah Subjek penelitian, perkiraan waktu, perkiraan biaya, penentuan variabel, penentuan parameter, ketersediaan kebutuhan alat dan bahan dengan 3 metode pengumpulan data, yaitu studi literature, observasi, dan wawancara.

3.1.2. Assessment Method

Metode yang digunakan untuk melakukan assessment adalah dengan melakukan uji penetrasi terhadap setiap lokasi penelitian yang memiliki layanan hotspot dan layanan tersebut selalu aktif, lalu hasil pengujian dari setiap lokasi penelitian diberi skor dengan sebuah format penilaian dimana penilaian tersebut akan dihitung nilai rata-rata nya dari seluruh hasil pengujian di semua lokasi penelitian.

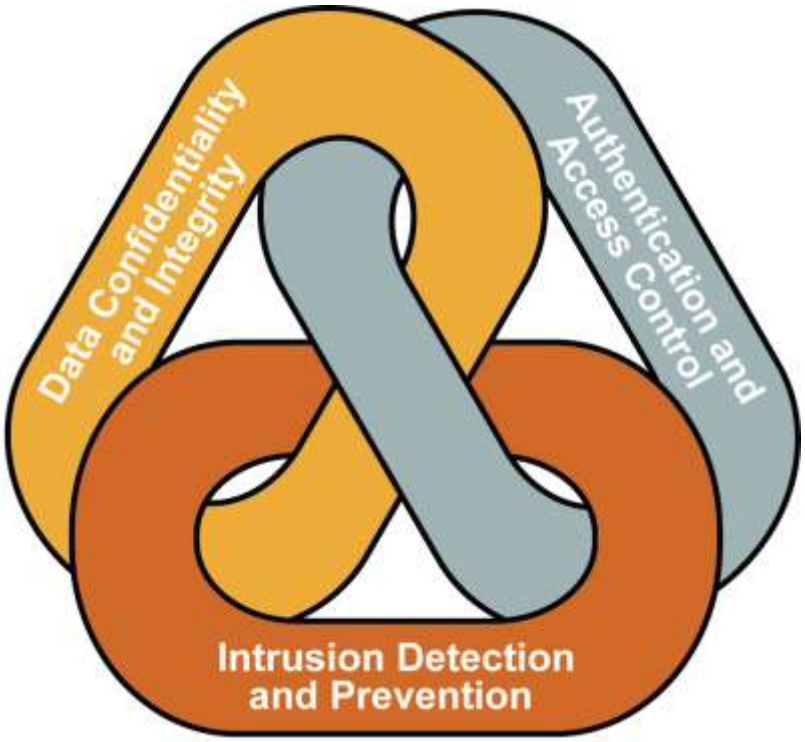
1. Uji Penetrasi

Proses pengujian penetrasi mengikuti kerangka kerja dari ISSAF. Kerangka kerja ini mempunyai 3 langkah utama dalam proses assessment, yaitu *Planning and Preparation, Assessment,* dan *Reporting and Clean up*.

Tahap *assessment* dalam kerangka kerja tersebut adalah tahapan khusus untuk melakukan pengujian terhadap *WLAN*, langkah WLAN Assessment ini terbagi menjadi 4 langkah pengujian, yaitu *Information Gathering, Analysis and Research, Exploit and Attack,* dan *Reporting and Presentation.* Setiap langkah dalam skema *WLAN Assessment* mempunyai proses yang berbeda dengan tujuan tersendiri.

Variabel yang ditentukan untuk setiap tahap WLAN Assessment menggunakan format yang berbeda dengan standar pengujian WLAN Assessment dari ISSAF dengan meninjau penentuan variabel yang digunakan pada standar ISSAF dinilai kurang mengikuti standar keamanan WLAN yang di implementasikan pada zaman sekarang yang sesuai dengan hasil observasi pada beberapa Kafe di sekitar wilayah Kelurahan Nagarawangi Kota Tasikmalaya.

Variabel yang digunakan dalam penelitian ini mengikuti hasil penelitian Refaat, dkk tentang "***Wireless Local Area Network Security Enhancement through Penetration Testing***" yang di publikasikan pada jurnal internasional IJCNCS pada tahun 2016 pada tingkat *Frame Level Wireless Attack,* seperti pada gambar 3.1:



Gambar 3.1. Aspek Keamanan Wireless(Siemens Company, 2008)

Tingkat Frame Level Wireless Attack meliputi 4 aspek utama keamanan jaringan wireless, yaitu:

a. *Confidentiality*
b. *Integrity*
c. *Authentication*
d. *Access Control*

4 aspek tersebut dikaji kembali sehingga menghasilkan beberapa variabel yang menjadi landasan penilaian tingkat keamanan yang tertera pada tabel 3.1. berikut:

Tabel 3.1. Aspek Keamanan Wireless

No	Aspek	Variabel
1	*Confidentiality*	Enkripsi Wireless
		Password Service Jaringan
2	*Integrity*	*WEP Crack*
		MITM
3	*Authentication*	*WEP*
		WPA/TKIP
		WPA/PSK
		Radius
		WPA AES+Radius
4	*Access Control*	*Mac-Filter*
		Implementasi Radius
		Audit Servis Jaringan

2. Perhitungan Hasil Pengujian

Perhitungan akan dilakukan secara dua tahap, yaitu perhitungan untuk setiap individu lokasi penelitian dan perhitungan secara keseluruhan. Perhitungan yang dilakukan pada setiap individu lokasi akan dilakukan setelah semua proses pengujian dilakukan dan hasil dari setiap parameter yang diukur didapatkan hasilnya. Parameter pengukuran tingkat keamanan tersebut adalah seperti pada tabel 3.2. berikut:

Tabel 3.2 Parameter Pengukuran Tingkat Keamanan Wireless

No	***Variabel***	***Parameter***	***Score***
Confidentiality			
1	*Wireless Encryption*	*No*	*-1*
2		*WEP*	*0*

3		*WPA/TKIP*	*+1*
4		*WPA/PSK*	*+2*
5		*WPA Enterprise*	*+3*
6	*Password Service Jaringan*	*Default*	*-1*
7		*Single Password*	*+1*
8		*Multiple Password*	*+2*
Integrity			
9	*WEP Crack*	*Enabled*	*-1*
10	*MITM*	*ARP Poison*	*-1*
11		*Packet Analyze*	*-1*
Authentication			
12	*WEP*	*64 bit*	*+1*
13		*128 bit*	*+2*
14		*152 bit*	*+3*
15	*WPA/TKIP*	*Short password, no complexity, no update periode*	*+2*
16		*Long password, no complexity, no update periode*	*+3*
17		*Long password, complex, no update periode*	*+4*
18		*Long password, complex, updated*	*+5*
19	*WPA/AES*	*Short password, no complexity, no update periode*	*+3*
20		*Long password, no complexity, no update periode*	*+4*
21		*Long password, complex, no update periode*	*+5*
22		*Long password, complex, updated*	*+6*
23	*Local Radius*	*Implemented (Default)*	*+4*
24		*Complex Username*	*+1*
25		*Short password, no complexity, no update periode*	*+1*
26		*Long password, no complexity, no update periode*	*+2*
27		*Long password, complex, no update periode*	*+3*
28		*Long password, complex, updated*	*+4*
29		*Limited Session*	*+1*
30		*Encrypted password*	*+1*
31	*Radius+WPA*	*Implemented*	*+12*
Access Control			
32	*Mac Filter*	*Implemented*	*+1*
33	*Radius*	*Implemented*	*+1*
34	*Network Service Audit*	*Telnet Port changed*	*+1*
35		*Telnet Access List*	*+1*

Keterangan Tabel 3.2:

a. Referensi parameter yang berhubungan dengan enkripsi wireless, adalah tingkat keamanan enkripsi yang di publikasi (Refaat, dkk. 2016).

b. Variabel Enkripsi wireless hanya akan menemukan 1 parameter dalam penilaian dengan artian jika seluruh parameter dalam variabel enkripsi wireless ditemukan dan dihitung jumlah score akan mendapat nilai 5, tapi dalam praktek hanya akan ditemukan 1 kondisi diantara 5 kondisi, karena parameter-parameter dari variabel enkripsi wireless tersebut merupakan suatu pilihan dari 5 pilihan.
c. Parameter nomor 1 diberi nilai "-1" jika keadaan sesuai parameter ditemukan karena sesuai dengan tingkat enkripsi yang di publikasi Refaat, dkk. 2016. Nilai "-1" ditentukan karena jika tanpa enkripsi, artinya aspek keamanan akan sangat berkurang.
d. Parameter nomor 2 diberi nilai 0 karena WEP adalah tingkatan paling rendah dari 5 tingkatan enkripsi wireless.
e. Parameter nomor 3 diberi nilai +1 karena WPA-TKIP adalah tingkatan ke-2 dari 5 tingkatan enkripsi wireless.
f. Parameter nomor 4 diberi nilai +2 karena WPA-AES adalah tingkatan ke-3 dari 5 tingkatan enkripsi wireless.
g. Parameter nomor 5 diberi nilai +2 karena WPA-AES adalah tingkatan ke-3 dari 5 tingkatan enkripsi wireless.
h. Parameter nomor 6 diberi nilai -1 karena jika password-password service dibuat default artinya akan sangat mengancam keamanan jaringan.
i. Parameter nomor 7 diberi nilai +1 karena password service diganti secara custom, tapi poin hanya satu karena seluruh service memiliki 1 password yang sama

j. Parameter nomor 8 diberi nilai +2 karena password service diganti secara custom, dan password setiap service yang ada dibuat berbeda.

k. Semua parameter pada aspek integrity akan dihitung untuk setiap parameter nya, dalam artian aspek integrity mempunyai 3 parameter dari 2 variabel, jika seluruh keadaaan parameter ditemukan maka hasil skor adalah "-3". Alasan nya adalah karena semua parameter yang ada pada aspek integrity merupakan suatu ancaman yang bersifat mengurangi sistem keamanan jaringan wireless.

l. Parameter nomor 9 diberi nilai -1 karena dalam referensi (Refaat, dkk. 2016) dalam table Frame level, implementasi WEP mengancam aspek integrity.

m. Parameter nomor 10 diberi nilai -1 karena serangan ARP Poison merupakan sebuah dapat menipu informasi arp table yang sesungguhnya.

n. Pengukuran dalam aspek authentication tidak dihitung untuk semua parameter, tapi parameter yang diukur tergantung dari jenis enkripsi yang diterapkan. Perbedaan nilai poin untuk setiap tipe enkripsi pada parameter dan poin terendah sampai tertinggi berdasarkan level enkripsi pada jaringan wireless (Refaat, dkk. 2016). Poin ditambah satu jika level enkripsi lebih tinggi, maka setiap variabel akan mempunyai nilai poin yang berbeda.

o. Variabel WEP hanya akan memilih 1 diantara 3 parameter sehingga nilai maksimal yang didapat adalah 3 dan nilai minimal adalah 1, perbedaan

nilai poin dikarenakan lebih banyak bit yang diterapkan, maka akan lebih memperlambat penyerang jika ada yang berusaha membobol kata kunci.

p. Variabel WPA-TKIP berada pada level lebih tinggi dari WEP, maka dengan parameter terendah nilai poin nya lebih tinggi dari parameter terendah pada WEP. Variabel WPA-TKIP hanya akan memilih 1 diantara 4 parameter sehingga nilai maksimal yang didapat adalah 5 dan nilai minimal adalah 2, perbedaan nilai poin didasarkan pada tingkat kerumitan kata kunci yang digunakan.

q. Variabel WPA-AES hanya akan memilih 1 diantara 4 parameter, perbedaan nilai poin didasarkan pada tingkat kerumitan kata kunci yang digunakan.

r. Variabel Local Radius jika di implementasi akan mendapat point 4 karena lebih tinggi dari WPA-AES dalam level enkripsi, selanjutnya setiap parameter dalam variabel local radius jika ditemukan dan terimplementasi akan di tambah sesuai poin yang tertera, jika tidak tidak akan ditambah. Maksimal poin yang akan didapat dari variabel Local Radius jika terimplementasi adalah 11 poin dengan kondisi parameter nomor 23, 24, 28, 29, dan 30 di implementasi.

s. Variabel Radius+WPA jika terimplementasi akan langsung mendapat 12 poin karena kehandalan dan tingkat keamanan nya.

t. Aspek access control mempunyai 4 variabel, dimana setiap parameter nya diacukan pada perangkat yang menajdi wireless station dengan pemberian

poin ditambah 1 jika terimplementasi dan tidak akan ditambah jika tidak terimplementasi satupun.

3.1.3. Preparation

Tahap ini terdiri dari informasi awal tempat penelitian, langkah-langkah yang direncanakan untuk proses penelitian, dan persiapan alat, software, dan berkas yang dibutuhkan untuk proses penelitian. Persiapan utama yang dipersiapkan dalam tahap ini adalah:

1. *Contact*

   Langkah ini akan melakukan identifikasi kontak secara Individu dengan semua Kedai yang menjadi lokasi penelitian untuk membicarakan maksud dan tujuan penelitian di setiap lokasi penelitian untuk mendapatkan informasi awal.

2. *Meeting*

   Langkah ini akan melakukan pertemuan secara formal dengan pihak lokasi penelitian untuk membicarakan scope dari pengujian dan metodologi yang akan digunakan untuk melakukan uji penetrasi.

3. *Agreement*

   Membuat perjanjian tertulis terkait pengujian penetrasi meliputi setiap langkah pengujian yang ditulis secara spesifik agar proses uji penetrasi bisa dilakukan secara formal dan untuk mencegah kesalah pahaman dan untuk masalah legalitas uji penetrasi selama proses pengujian dan setelah pengujian selesai.

Perjanjian ini adalah langkah penting yang biasa disebut *ROE (Rules of Engagement)* yang berisi ruang lingkup pengujian, dan mekanisme pengujian. Adanya perjanjian ini sesuai dengan yang tertera pada standar *ROE* uji penetrasi yang diterbitkan dan di revisi oleh *PTES(Penetration Testing Execution Standard)* pada websitenya pada tahun 2014.

4. Alat dan Bahan

Peralatan dan bahan yang dipersiapkan untuk melakukan uji penetrasi ini adalah:

a. Laptop dan Komputer

   Laptop digunakan sebagai media melakukan uji penetrasi. Komputer digunakan untuk melakukan riset pengujian tools sebelum dilakukan di lapangan.

b. *USB Wireless*

   USB Wireless digunakan untuk melakukan riset pengujian tools sebelum dilakukan di lapangan.

c. *Access Point*

   Access Point digunakan untuk melakukan riset pengujian tools sebelum dilakukan di lapangan.

d. *Tools*

   Tools yang digunakan untuk melakukan uji penetrasi terhadap sistem keamanan wireless dalam penelitian ini dapat dilihat pada tabel 3.3 berikut:

   Tabel 3.3. *Tools* untuk *Wireless Penetration Testing*

No	*Tools*
1	*Airmon-ng*
2	*Airodump-ng*
3	*Aireplay-ng*
4	*Aircrack-ng*
5	*Mac Changer*
6	*Access Point/Wireless Router Default Password List*
7	*Crunch*
8	*Mac Changer*
9	*Wireshark*
10	*Ettercap*
11	*Network Miner*
12	*Password List*
13	*Browser*
14	*Telnet*
15	*Angry IP Scanner*

3.2. *Assessment*

Langkah assessment mengikuti metodologi uji penetrasi terhadap *WLAN* dari *ISSAF* yang meliputi 4 langkah, yaitu *Information Gathering, Analysis and Research, Exploit and Attack,* dan *Reporting and Presentation.* Berikut adalah penjelasan dari langkah-langkah tersebut:

3.2.1.Information Gathering

Tahap information gathering mengumpulkan berbagai informasi terkait parameter-parameter pengukuran tingkat keamanan *wireless* meliputi:

1. Topologi Jaringan

   Topologi jaringan yang ada digunakan untuk menganalisa kemungkinan sistem keamanan yang digunakan. Data topologi jaringan didapatkan dengan cara observasi dan wawancara secara langsung.

2. Jumlah *WLAN* untuk Tamu

Jumlah *WLAN* yang ada akan sangat mempengaruhi hasil dari pengukuran tingkat keamanan, maka dilakukan pengecekan jumlah *WLAN* yang disediakan oleh lokasi penelitian yang diperuntukan bagi tamu.

Data jumlah *WLAN* dilakukan dengan cara wawancara dan melakukan scanning dengan tool *airmon-ng* untuk merubah wireless card pada laptop menjadi mode monitor dan *airodump-ng* untuk melakukan *scanning* terhadap *wireless* yang aktif disekitar lokasi penelitian sebagai verifikasi.

3. *SSID*

   SSID dari *WLAN* yang aktif dikumpulkan dengan cara melakukan scanning menggunakan *tools airmon-ng* dan *airodump-ng*. *SSID* digunakan sebagai acuan dari pemilihan *BSSID* dari *access point* yang memang berasal dari satu subjek atau satu lokasi penelitian.

4. *Channel*

   Channel diperlukan untuk proses perekaman paket-paket wireless yang nantinya akan digunakan dalam proses *cracking* enkripsi *wireless* dan proses mendapatkan *WPA Handshake*. *Channel* didapatkan dengan cara scanning menggunakan *tools airmon-ng* dan *airodump-ng*.

5. *Access Point BSSID*

   Mac address dari sebuah *access point* atau *access point bssid* adalah parameter jaringan yang banyak dibutuhkan dalam proses pengujian pada tahap *Exploit and Attack*. *Access point BSSID* didapatkan dengan melakukan scanning yang dicocokan dengan *ESSID* dari access point itu sendiri.

6. *Client* BSSID

Client BSSID adalah *mac address* dari pengguna jaringan atau tamu yang dalam penelitian ini digunakan untuk proses mendapatkan *wpa handshake*. *Client BSSID* didapatkan dengan cara scanning dengan tools *airmon-ng* dan *airodump-ng*.

7. *Wireless Encryption*

   Tipe *wireless encryption* diperlukan untuk melakukan *password cracking*. Tipe *wireless encryption* didapatkan dengan melakukan *scanning*.

8. *Service Scan*

   Service scan dilakukan untuk mengecek ketersediaan servis jaringan dalam sebuah access point. *Service* yang di cek adalah servis web dengan *protocol* http dan service *telnet*. Service web dan telnet dipilih karena merupakan jalan untuk masuk pada mode konfigurasi access point. *Scanning* dilakukan dengan *tool nmap* dan *angry ip scanner*.

9. *Radius User Profile* (Jika di implementasikan)

   Radius user profile berisi tentang berbagai parameter jaringan yang berpengaruh langsung terhadap implementasi setiap user jaringan. Jika radius diimplementasikan di lokasi penelitian, maka *user profile* didapatkan dengan cara *social engineering*.

   Parameter yang dikumpulkan dalam radius user profile meliputi semua parameter pada variabel *Local Radius* yang tertera pada parameter nomor 22 hingga nomor 29 dalam tabel 3.2.

3.2.2.Analysis and Research

Fase *Analysis and Reasearch* melakukan analisis dan riset terhadap jenis serangan yang akan dilakukan berdasarkan hasil dari fase *Information Gathering.*

1. *Packet Capture*

   Serangan ini melakukan pengumpulan paket-paket data jaringan wireless yang lewat dengan melakukan sniffing. *Packet capture* memerlukan beberapa informasi dasar, yaitu *SSID, Access Point BSSID, Channel*. *Tools* yang digunakan dalam melakukan *packet capturing* adalah *airmon-ng* dan *airodump-ng.*

   Airmon-ng digunakan untuk merubah *wireless card* menjadi mode monitor dengan memasukan perintah seperti pada table 3.4. berikut:

Tabel 3.4. Opsi Perintah Airmon-ng

No	Script	Fungsi
1	`airmon-ng check kill`	Mematikan semua service yang menghalangi
2	`airmon-ng start <nama_interface>`	Merubah mode wireless card menjadi mode monitor
3	`iwconfig`	Verifikasi perubahan mode wireless card

Airodump-ng digunakan untuk merekam suatu percakapan jaringan wireless dengan format:

"*airodump-ng <nama_interface_monitor> <option>*".

Format <*option*> dalam *script* tersebut adalah seperti pada table 3.5 berikut:

Tabel 3.5. Opsi Perintah Airodump-ng

No	Script	Fungsi

1	*airodump-ng –bssid <bssid access point>*	Untuk melakukan perekaman data yang lewat berdasarkan bssid access point tertentu
2	*airodump-ng –c <channel>*	Untuk melakukan perekaman data berdasarkan channel tertentu
3	*airodump-ng –w <nama file>*	Untuk menyimpan data perekaman dan memberi nama file tersebut

2. *Service Scan*

Service scan dilakukan terhadap *access point* untuk melakukan pengecekan aktifnya servis *web* dan *telnet* untuk masuk ke dalam mode konfigurasi *access point*. *Service scan* menggunakan tool *nmap* dengan format:

"*nmap –p 80,21 <ip address>*"

3. *Packet Analyze*

Packet analyze menggunakan 2 tools, yaitu *wireshark* dan *network miner*. Wireshark digunakan bersamaan dengan Ettercap, ketika dalam pemantauan pada wireshark dinilai data yang didapat mealui teknik *sniffing* sudah cukup, maka *file* penyadapan akan disimpan dengan ekstensi ".*cap*". File tersebut akan di buka kembali dengan tool network miner yang dapat melakukan klasifikasi paket jaringan secara rinci.

3.2.3.Exploit and Attack

1. *WEP Crack*

WEP crack menggunakan tools *aircrack-ng* dengan format:

"*aircrack-ng <nama_file>*"

File yang damaksud adalah file hasil perekaman menggunakan tool airodump-ng.

2. *Deatuthentication Attack*

Deauthentication attack dilakukan untuk memperoleh paket *wpa handshake*. Tool yang digunakan adalah airodump-ng untuk merekam paket, dan *aireplay-ng* dengan format berikut:

"*aireplay-ng <option> <replay interface>*"

Replay interface adalah nama interface dalam mode monitor, dan opsi adalah seperti pada table 3.6 berikut:

Tabel 3.6. Opsi Perintah Aireplay-ng

No	Script	Fungsi
1	`Aireplay-ng -0 <1-10> <interface>`	-0 adalahOpsi untuk memilih serangan deauthentication, dan angka adalah jumlah serangan yang akan dikirim
2	`Aireplay-ng -0 1 -a <bssid> <interface>`	-a adalah opsi untuk menambahkan bssid access point tertentu
3	`Aireplay-ng -0 1 -a <bssid> -c <bssid> <interface>`	-c adalah opsi untuk memasukan bssid dari salah satu client yang terhubung

3. *WPA Crack*

WPA crack dilakukan setelah mendapatkan *wpa handshake*. Ada dua opsi yang digunakan untuk melakukan *WPA cracking*, yaitu dengan memanfaatkan file *wordlist* dan menggunakan tool *crunch*. *Crunch* berfungsi untuk melakukan *brute force* secara random dengan format:

"*crunch <min> <max> [option]*"

<*Min*> adalah jumlah karakter minimal yang dicari, <*max*> adalah jumlah karakter maksimal, dan *[option]* adalah opsi karakter yang akan dicari. Pengujian ini menggunakan format minimal 8 karakter, maksimal 20 karakter dengan opsi karakter yang ada pada nama kedai ditambah karakter-karakter yang ada pada kata kedai, kafe, dan coffee ditambah angka 0-9. Contoh, nama kedai adalah Java, maka opsi karakternya adalah "javakedaicoffee0123456789", maka perintah dalam crunch adalah

"*crunch 8 20 javakedaicoffee0123456789*"

Crunch hanyalah untuk melakukan *brute force*, proses *cracking* dilakukan dengan tool *aircrack-ng* dengan format dasar:

"*aircrack-ng <option> <file hasil rekaman>*"

Opsi yang digunakan adalah seperti pada table 3.7 berikut:

Tabel 3.7. Opsi Perintah Aircrack-ng

No	Script	Fungsi
1	`Aircrack-ng –b <bssid> <file>`	-b adalah opsi untuk menjadikan mac address dari suatu access point sebagai target
2	`Aircrack-ng –w <wordlist> <file>`	-w adalah opsi untuk melakukan cracking berdasarkan wordlist yang diikuti nama file wordlist tersebut beserta lokasi penyimpanan wordlist tersebut

Penggunaan gabungan dari *aircrack-ng* dan *crunch* dilakukan dengan format masing-masing *tools* secara menyeluruh serta dipisahkan dengan karakter "|", contohnya:

" `crunch 8 20 javakedaicoffee0123456789|aircrack-ng –b 01:23:45:6A:3B "Home/file.cap"` "

4. *Brute Force Service*

Brute force dilakukan setelah melakukan *ip scanning* dengan *arp*, setelah mendapatkan semua *ip address* beserta *mac address* yang aktif, akan dicari yang *mac-address* nya sama dengan hasil *scanning* menggunakan *airodump-ng*.

Brute force service memanfaatkan daftar *password* dari service web dan service telnet. Misalnya password default untuk memasuki mode konfigurasi *wireless router A* pada layanan *WEB* adalah username=”admin” dan password=”admin”.

5. *ARP Poison*

ARP Poison dilancarkan untuk menipu informasi *arp table* yang ada pada client sehingga laptop penyerang dianggap sebagai tujuan transmisi. *ARP Poison* dilancarkan menggunakan tool *Ettercap* dengan cara melakukan scanning terhadap daftar *ip* dan *mac address* yang aktif, lalu menentukan target 1 dan target 2. Target 1 adalah target yang menjadi tujuan sesungguhnya dari pengiriman transmisi jaringan dari target 2 yang dalam penelitian ini ditetapkan target 1 adalah access point, dan target 2 adalah user atau tamu.

3.2.5.Reporting and Presentation

Tahap ini berisi tentang mekanisme pelaporan hasil pengujian penetrasi dan proses pembersihan semua hal yang tersisa selama proses pengujian yang dapat membahayakan sistem.

1. *Reporting*

Laporan terdiri dari 2 jenis yaitu laporan verbal dan laporan akhir.

a. Laporan Verbal

Mekanisme laporan verbal adalah langsung mendiskusikan hasil pengujian apabila ada celah keamanan yang bersifat fatal yang ditemukan selama proses pengujian. Celah keamanan ini akan didiskusikan berikut penanganan yang harus dilakukan agar celah keamanan dapat ditutup.

b. Laporan Akhir

Laporan akhir adalah laporan keseluruhan yang meliputi semua hal terkait pengujian yang terdiri dari 7 poin utama, yaitu:

a) Ringkasan manajemen pengujian penetrasi
b) Hal-hal yang berkaitan dalam ruang lingkup maupun diluar ruang lingkup pengujian.
c) Tools yang digunakan
d) Tanggal dan waktu untuk setiap proses pengujian
e) Hasil pengujian spesifik dari setiap proses pengujian baik dalam serangan pasif maupun serangan aktif untuk setiap poin yang ada pada tabel 3.1.
f) Semua vulnerabilitas yang ditemukan
g) Rekomendasi langkah penanganan yang perlu dilakukan

3.2.6. Clean Up and Destroy Artifact

Tahap ini melakukan pembersihan dari semua perubahan yang terjadi terhadap sistem selama proses pengujian dilakukan, langkah yang dilakukan adalah:

1. Jika serangan *DDOS* masih berlangsung maka akan dimatikan
2. Jika terjadi perubahan konfigurasi pada *Access Point* maka akan dikembalikan seperti semula
3. Jika proses perekaman data yang di broadcast *Access Point* masih berlangsung maka akan dihentikan
4. Jika hasil pengukuran tingkat keamanan sudah didapat, semua file yang didapatkan melalui proses uji penetrasi akan di kembalikan pada Kedai atau Kafe.