ANALISIS KEAMANAN JARINGAN PADA *WIRELESS LOCAL AREA NETWORK* TERHADAP SERANGAN *BRUTE FORCE* MENGGUNAKAN METODE *PENETRATION TESTING*

Rozi Dayan, Yusuf Muhyidin, Dayan Singasatia
Program Studi Teknik Informatika S1, Fakultas Teknik, Sekolah Tinggi Teknologi Wastukancana
Jl. Cikopak No.53, Sadang, Purwakarta, Jawa Barat, Indonesia
rozidayan02@wastukancana.ac.id

ABSTRAK

Pentingnya informasi dan komunikasi saat ini tidak bisa diabaikan dan menjadi kebutuhan utama bagi banyak orang. Mereka menginginkan akses informasi yang mudah dan cepat di mana pun mereka berada. Salah satu teknologi yang memenuhi kebutuhan tersebut adalah teknologi nirkabel. Dalam wawancara dengan tim IT, diketahui bahwa Politeknik Bhakti Asih dalam hal nirkabel masih dalam proses pembangunan. Oleh karena itu, Politeknik Bhakti Asih Purwakarta perlu menganalisis keamanan jaringan mereka untuk memastikan bahwa sistem keamanan jaringan mereka, terutama jaringan nirkabel, dapat diandalkan. Untuk itu, mereka membutuhkan penggunaan alat standar dalam analisis, yaitu Metode *Penetration Testing*. Hasil pengujian menunjukkan bahwa titik akses pertama, yaitu titik akses di ruangan yayasan, memiliki kata sandi yang mudah ditebak dan rentan terhadap serangan. Oleh karena itu, perlu adanya penanganan yang lebih baik dan penggunaan frase sandi yang lebih kuat.

Kata kunci: *Analisis, Keamanan Jaringan, Wireless, Brute Force, Penetration Testing*

1. PENDAHULUAN

Saat ini, komunikasi dan informasi sangat penting. Beberapa individu bahkan memerlukan akses informasi kapan saja dan di mana saja. Karena teknologi nirkabel telah membantu memenuhi kebutuhan ini, manusia harus terus meningkatkan jumlah dan kualitas teknologi komunikasi. Namun, karena semakin banyak orang yang dapat mengakses internet, semakin banyak kesempatan untuk tindakan kriminal seperti pencurian data atau peretasan jaringan. Serangan tersebut dapat dilakukan untuk mendapatkan sumber daya, mengubah konfigurasi sistem jaringan, atau mengubah data.

Password Cracking adalah istilah yang merujuk pada sekumpulan teknik yang digunakan untuk mendapatkan password dari sebuah sistem data yang dilindungi dengan password. Prosesnya berfokus pada mendapatkan password dari sistem yang dilindungi tersebut. Salah satu metode yang digunakan dalam Password Cracking adalah Footprinting, yang kemudian digunakan untuk membuat kombinasi password menggunakan metode brute-force attack [1].

Sebagai bagian dari sistem, keamanan jaringan komputer sangat penting untuk menjaga validitas dan integritas data serta menjamin ketersediaan layanan bagi pengguna.Sistem keamanan jaringan komputer harus dilindungi dari serangan dan pemindaian oleh orang yang tidak berhak.

Saat ini, sistem deteksi penyusup jaringan dapat mendeteksi berbagai jenis serangan, tetapi mereka tidak dapat mengambil tindakan tambahan.Selain itu, ketika administrator tidak menggunakan sistem, sistem tidak berinteraksi dengannya. Ini tidak efektif, terutama saat sistem dalam keadaan kritis [2].

Politeknik Bhakti Asih Purwakata terletak dikota Purwakarta Provinsi Jawa Barat, saat ini mengunakan Jaringan yang terdiri dari 5 perangkat *wireless* yang mencakup seluruh bidang di kantor dengan menggunakan keamanan WPA2-PSK. *wireless local area network* (WLAN) yang digunakan lebih sering mengalami kendala pada sistem kamanan jaringan dibandingkan menggunakan jaringan LAN. Disini penulis akan melakukan penelitian yaitu melakukan peretasan terhadap perangkat jaringan *wireless local area network* yang ada di Politeknik Bhakti Asih Purwakarta karena perangkat yang ada di Politeknik Bhakti Asih itu sendiri masih dalam tahap pembangunan jaringan baru, sehingga tingkat keamanan yang ada masih rentan dalam peretasan oleh pihak asing dan peneliti akan melakukan eksploitasi untuk memberikan solusi jika serangan berhasil dilakukan.

2. TINJAUAN PUSTAKA

2.1. Kalilinux

Kali linux adalah salah satu distribusi Linux tingkat lanjut untuk Penetration Testing dan audit keamanan. Kali Linux merupakan pembangunan kembali BackTrack Linux secara sempurna, mengikuti sepenuhnya kepada standar pengembangan Debian. Semua infrastruktur baru telah dimasukkan ke dalam satu tempat, semua tools telah direview dan dikemas, dan kami menggunakan Git untuk VCS nya [3].

2.2. *Brute Force*

Algoritma brute force adalah algoritma yang memecahkan masalah dengan sangat sederhana, langsung dan dengan cara yang jelas/lempang. Penyelesaian permasalahan kode cracking dengan menggunakan algoritma brute force akan menempatkan dan mencari semua kemungkinan kode dengan masukan karakter dan panjang kode tertentu

tentunya dengan banyak sekali kombinasi kode. Algoritma brute force adalah algoritma yang lempang atau apa adanya. Pengguna hanya tinggal mendefinisikan karakter set yang diinginkan dan berapa ukuran dari kodenya. Tiap kemungkinan kode akan di generate oleh algoritma ini [4].

2.3. Keamanan Jaringan

Menurut Amarudin dan Ulum, keamanan jaringan ialah salah satu isu terpenting saat mengimplementasikan jaringan komputer. Beberapa jaringan komputer mengalami kendala akibat kecerobohan administrator jaringan dalam membangun jaringan komputer tersebut. Karena kelalaian ini, dimungkinkan bagi peretas untuk mengakses dan merusak jaringan yang dibangun. Keamanan jaringan atau sistem informasi adalah "proses melindungi aset informasi, termasuk melindungi kerahasiaan, integritas, dan ketersediaan aset informasi tersebut" [5].

Menurut Munawar dan Putri, keamanan jaringan komputer mengacu pada perlindungan perangkat keras, perangkat lunak, dan sumber informasi sistem komputer agar tidak secara tidak sengaja atau berbahaya dihancurkan, dimodifikasi atau dirusak oleh pelanggaran keamanan, sehingga sistem komputer terus berfungsi. bekerja dengan andal dan melakukan layanan IT secara teratur [6].

2.4. Hostpot

Menurut Qirom dan Sungkar [7], Hotspot adalah area dimana seorang client dapat terhubung dengan internet secara wireless (nirkabel atau tanpa kabel) dari PC, Laptop, notebook ataupun gadget seperti handphone dalam jangkauan radius kurang lebih beberapa ratus meteran tergantung dari kekuatan frekuensi atau signal nya.Hotspot adalah "suatu sistem yang memberikan fitur autentikasi pada user yang akan mengakses suatu jaringan. Bila user tersebut ingin terhubung ke jaringan tersebut maka user tersebut harus memasukkan username dan password terlebih dahulu.

Menurut Angga Syaputera dkk [8], Hotspot adalah atau area hotspot adalah tempat khusus yang disediakan untuk mengakses internet mengunakan peralatan Wi-fi. Umumnya layanan hotspot bersifat gratis. Dengan berbekal laptop atau PDA maka koneksi internet dapat dilakukan secara cuma-cuma. Biasanya pengguna terlebih dulu harus melakukan registrasi kepenyedia layanan hotspot untuk mendapatkan login dan password. Kemudian pengguna dapat mencari area hotspot, seperti pusat perbelanjaan, kafe, hotel, kampus, sekolahan, bandara udara, dan tempattempat umum lainnya. Proses otentikasi dilakukan ketika browser diaktifkan.

3. METODE PENELITIAN

3.1. *Penetration Testing*

Penetration testing atau bisa disebut juga dikenal sebagai ethical hacking, merupakan suatu pendekatan untuk menguji dan mengevaluasi tingkat keamanan sistem komputer atau jaringan dengan melakukan percobaan serangan peretasan secara sistematis dan beretika [9]

3.2. *Information Gathering*

atau bisa disebut Pengumpulan Informasi memiliki peranan penting dalam pengujian. Seseorang dapat mengumpulkan informasi tersebut secara manual atau dengan menggunakan alat layanan (seperti teknik analisis kode sumber halaman web.) yang dapat diakses secara gratis melalui internet. Alat-alat ini membantu mengumpulkan berbagai informasi seperti nama tabel, versi database, perangkat lunak, perangkat keras, dan bahkan plugin pihak ketiga yang terpasang, dan lain sebagainya.

3.3. *Theat modelling*

Pada tahap ini penguji akan mencoba melakukan percobaan serangan untuk mendapatkan informasi username dan password.

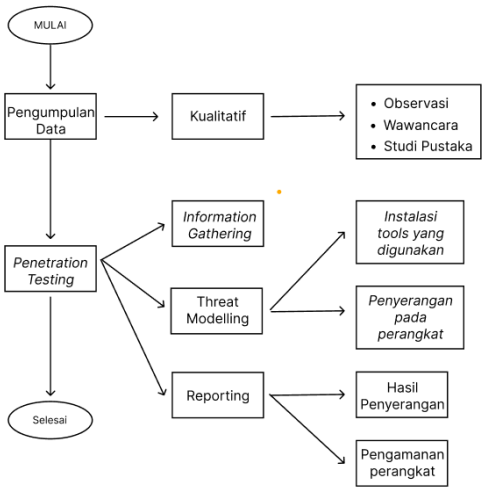
3.4. *Reporting*

Pada tahap pelaporan, setelah pengujian dilakukan, penguji menyiapkan laporan akhir yang menjelaskan segala sesuatu tentang sistem. Akhirnya laporan dianalisis untuk mengambil tindakan Penyesuaian untuk melindungi sistem target dapat dilihat pada gambar 1. Di bawah untuk tahapan penetration testing.

Gambar 1. Tahapan penetration testing

3.5. Alur Penelitian

Dalam melakukan penelitian ini, Peneliti menggunakan pendekatan penelitian kualitatif yang bersifat deskriptif. Pendekatan ini dipilih karena fokus permasalahannya adalah untuk menggambarkan atau mendeskripsikan keadaan subjek atau objek akan diteliti. Berikut gambar 2. adalah tahapan analisis sistem jaringan yang digunakan.



Gambar 2. Alur dan tahapan penelitian

4. HASIL DAN PEMBAHASAN

4.1. Hasil Pengumpulan Data

Dalam penelitian ini, peneliti mengadopsi pendekatan kualitatif untuk mengumpulkan data melalui tiga metode, yaitu observasi, wawancara, dan studi pustaka. Berikut adalah hasil dari pengumpulan data tersebut.

4.2. Obesrvasi

Hasil observasi di Politeknik Bhakti Asih Purwakarta menunjukkan penggunaan berbagai tipe router TP-LINK, seperti TL-WR940N hingga TL-WR941N, dengan semua perangkat Wi-Fi masih menggunakan keamanan WPA2-PSK, bahkan beberapa masih menggunakan keamanan WEP. Penelitian ini hanya akan menguji dan menyerang perangkat yang menggunakan keamanan WPA2-PSK, tanpa melibatkan perangkat dengan jenis keamanan lainnya.

4.3. Wawancara

Hasil wawancara dengan pihak IT Politeknik Bhakti Asih Purwakarta menyatakan bahwa dalam penelitian yang akan dilakukan, hanya beberapa perangkat Wi-Fi yang ada di beberapa ruangan yang akan diuji, dengan batas maksimal 2 perangkat untuk penelitian dan pengujian. Penulis mencari informasi minimal tentang perangkat yang akan diteliti dan diuji untuk membuat wordlist yang akan digunakan dalam tahap penyerangan atau pengujian perangkat Wi-Fi. Hal ini bertujuan untuk mempermudah proses tahap eksploitasi perangkat nantinya.

4.4. Studi Pustaka

Peneliti memperkuat penelitian ini dengan melakukan studi pustaka yang mencakup referensi dari buku, jurnal, dan tugas akhir terkait konsep dan teknik penyerangan menggunakan metode penetration testing.

4.5. *Information Gathering*

Dari tahap information gathering, penulis telah memperoleh informasi mengenai kebutuhan pengguna dan perangkat yang akan digunakan dalam tahap selanjutnya penelitian ini. Berikut adalah kebutuhan yang diperlukan untuk melakukan penelitian ini:

4.6. Kebutuhan Perangkat Keras

Tabel 1. Kebutuhan *Hardware*

No	Perangkat Keras	Spesifikasi
1.	Laptop	a. Processor Inter Core i3 b. RAM 8 GB DDR4 c. SSD 256 GB

4.7. Kebutuhan Perangkat Lunak

Tabel 2. Kebutuhan Software

No	Perangkat Keras	Spesifikasi
1.	Laptop	a. Processor Inter Core i3 b. RAM 8 GB DDR4 c. SSD 256 GB

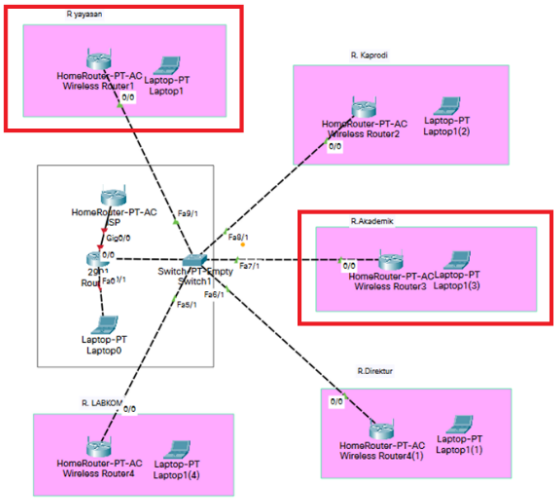
4.8. Identitas Perangkat Yang di Uji

*Access poin*t TP-LINK tipe TL-WR940N dan TL-WR941HP

Wireless router ini dilengkapi dengan tiga antena 5dBi, TL-WR940N dan TL-WR941HP dapat meningkatkan transmisi sinyal nirkabel dan penerimaan. Dengan 4 port Ethernet cepat, ia menyediakan Wi-Fi yang andal dan koneksi kabel untuk rumah berukuran sedang, membiarkan keluarga Anda menikmati Wi-Fi cepat bersama di setiap smartphone, tablet, dan laptop.

4.9. Topologi Jaingan Target

Dalam tahap *information gathering* ini pun, peneliti mendapatkan informasi terkait skema topologi yang ada, dan peneliti mengambil informasi mulai dari nama perangkat yang akan di uji serta perangkat mana saja yang akan dilakukan pengujian, karena peneliti diberikan izin oleh pihak Politeknik Bhakti Asih Purwakarta dalam penelitian dan pengujian ini hanya diberikan 2 ruangan yang terdapat perangkat *Wiresless Fidelity (Wi-Fi)*, penelti akan menguji perangkat jaringan yang berada di ruangan Yayasan serta ruangan Akademik. Berikut gambar topologi jaringan dapat dilihat pada gambar 3. Di bawah ini.



Gambar 3. Topologi jaringan target penelitian

4.10. *Threat Modelling*

Dari tahapan sebelumnya informasi yang dikumpulkan akan di lanjutkan pada tahap ini, penulis akan melakukan simulasi penyerangan untuk mendapatkan *password* dari wireles. Dalam hal ini penulis akan, mensimulasikan diri sebagai peretas di dalam Jaringan Politeknik Bhakti Asih Purwakarta. Penyerangan akan di lakukan terhadap perangkat *wireless* yang sudah di amankan mengunkan WPA/WPA2 PSK. Berikut langkah yang dilakukan oleh peneliti dalam pengujian serta peretasan terhadap perangkat jaringan.

4.11. *Instalasi Tools Aircrack-ng*

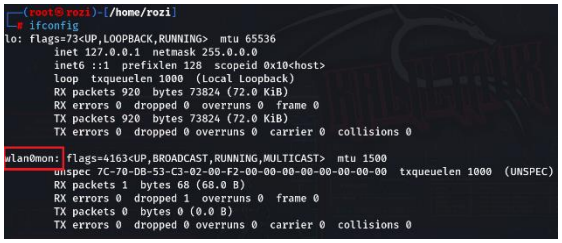
Dalam tahap pertama untuk melakukan eksploitasi perangkat jaringan yang akan dilakukan

oleh peneliti yaitu melakukan instalasi *Tools* yang akan digunakan dalam tahap penyerangan ini. Instalasi tools aircrack ditunjukan pada gambar 4. Di bawah ini.

Gambar 4. Installasi tools

4.12. Mengaktifkan Mode Monitoring interface Wlan

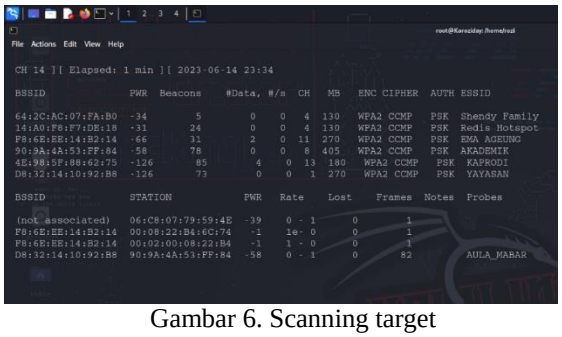
Dalam tahap mengaktifkan mode monitoring, peneliti melakukan perintah pada tools aircrack yaitu dengan perintah *aircrack-ng start wlan0* maka interface akan berubah menjadi interface wlan0mon yang berarti berhasil menjadi interface monitor mode. Monitor mode berhasil di aktifkan dapat dilihat pada gambar 5. Di bawah ini.



Gambar 5. Monitor Mode

4.13. Scanning Wireless

Dalam tahap ini peneliti akan melakukan *scanning* untuk mendapatkan informasi dari target yang akan dilakukan pengujian penetration dengan teknik *Brute force*. Dalam melakukan *scanning wireless* ini, peneliti memasukan perintah "airmon-ng wlan0mon" untuk mendapatkan informasi terkait jaringan *wireless* apa saja yang ada di ruang lingkup pengujian. Hasil scanning perangkat target ditunjukan pada gambar 6. Di bawah ini.



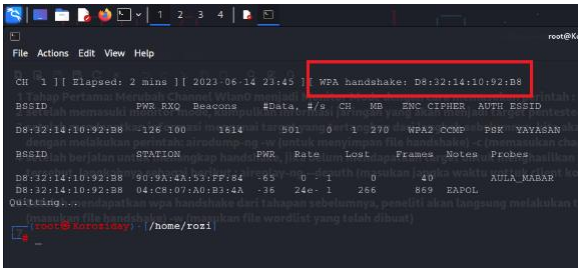
Gambar 6. Scanning target

4.14. Proses Capturing Handshake pada target pertama (Ruang Yayasan)

Proses ini merupakan tahap yang sangat berpengaruh pada langkah berikutya, pada proses capturing handshake ini peneliti menggunakan informasi yang terdapat pada proses sebelumnya yaitu scanning wireless yaitu informasi BSSID, CH serta ESSID untuk melanjutkan tahap atau berikutnya, dan proses ini akan menghasilkan output berupa file .cap yang digunakan pada tahapan cracking untuk memperoleh informasi password yang digunakan oleh perangkat target yang sedang di uji. Ada beberapa tahapan untuk Proses capturing handshake dapat dilihat pada gambar 7, 8, 9 di bawah ini.

Gambar 7. *Dump ke-target pertama*

Gambar 8. Menunggu *handshake Ter-capture*



Gambar 9. *Handshake berhasil Ter-capture*

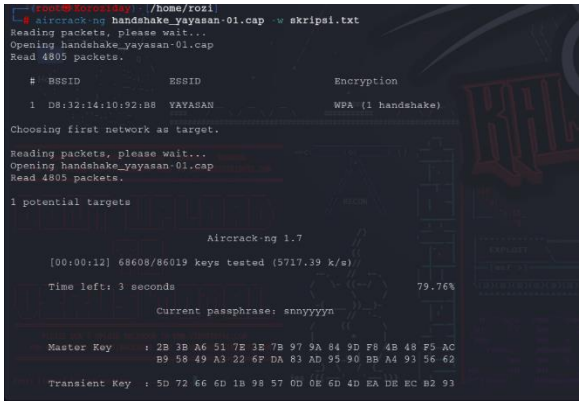
4.15. Brute Force Attack

Sebelum melakukan proses selanjutnya peneliti akan mempersiapkan bahan untuk melakukan penyerangan menggunakan teknik penyerangan Brute Force Attack. Yang perlu di siapkan dalam penyerangan ini yaitu tools aircrack yang sudah di install sebelumnya serta file wordlist yang sudah dibuat untuk melancarkan penyerangan brute force, fille wordlist yang di buat berisi kemungkinan password yang digunakan oleh perangkat uji atau target yang akan diserang, brute force akan bekerja dengan menyandingkan tools aircrack dengan file wordlist yang sudah di buat, secara otomatis sistem Kalilinux akan bekerja dalam mencari kemungkinan password yang digunakan oleh perangkat target

4.16. Proses Cracking Target Pertama (Ruang Yayasan)

Setelah mendapatkan file *handshake* yang didapatkan pada tahap sebelumnya, untuk langkah cracking ini peneliti akan melakukan teknik *brute force* menggunakan *Tools* aircrack-ng serta menyiapkan file wordlist yang sudah peneliti buat untuk mendapatkan *password* dari perangkat yang diuji. Wordlist sendiri merupakan sebuah kumpulan kata acak untuk di gunakan dalam penyerangan menggunakan metode *brute force* yang dilakukan ini.

perintah yang digunakan yaitu "aircrack-ng *"file handshake.cap" –w "file wordlist""*. Dalam proses cracking target pertama tahapan ditunjukan pada gambar 10 & 11.



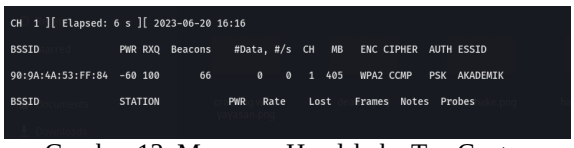
Gambar 10. Proses *Cracking* target pertama

Gambar 11. Informasi password berhasil didapatkan

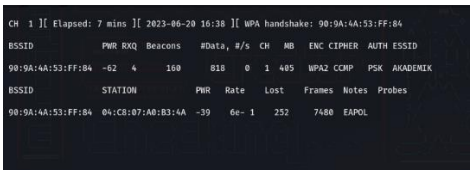
4.17. Proses Capturing Handshake pada target kedua (Ruang Akademik)

Seperti yang sudah dilakukan pada proses *capturing handshake* pada perangkat pertama yaitu perangkat yang ada di ruangan yayasan, semua perintah yang dilakukan sama hanya saja target yang akan di uji tidak akan memiliki BSSID yang sama dan channel yang serupa, maka dari itu peneliti memasukan perintah yang sama dengan proses yang sebelumnya hanya merubah BSSID target dan Channel target yang akan di lakukan pengujian. Perintah yang dilakukan yaitu "airodump-ng –bssid –channel –write wlan0mon". proses capturing handshake pada target kedua ditunjukan pada gambar 12, 13, 14 di bawah ini.

Gambar 12. Dump Ke Target Kedua



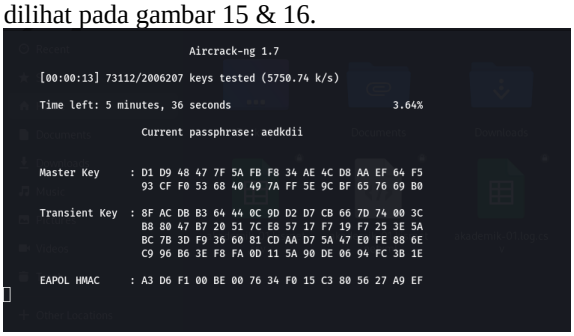
Gambar 13. Menungu Handshake Ter-Capture



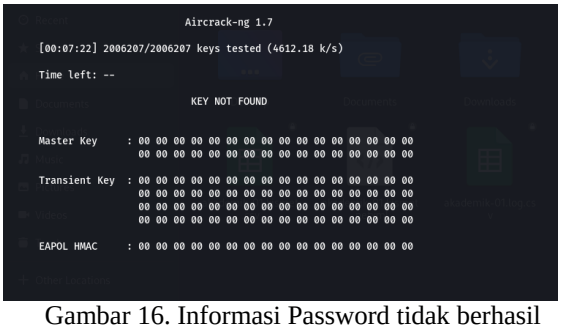
Gambar 14. Handshake Berhasil Ter-capture

4.18. Proses Cracking Target Kedua (Ruang Akademik)

Sama seperti Proses cracking sebelumnya, Setelah mendapatkan file *handshake* yang di dapatkan pada tahap sebelumnya, untuk langkah cracking ini peneliti akan melakukan teknik *brute force* menggunakan *Tools* aircrack-ng serta menyiapkan file wordlist yang sudah peneliti buat untuk mendapatkan *password* dari perangkat yang akan dilakukan pengujian ini. perintah yang digunakan yaitu "aircrack-ng *"file handshake.cap" –w "file wordlist""*. hasil dari cracking pada target kedua dapat dilihat pada gambar 15 & 16.



Gambar 15. Proses *Cracking* Target Kedua



Gambar 16. Informasi Password tidak berhasil didapatkan

4.19. Reporting

Dari pengujian sebelumnya peneliti memperoleh hasil dari penyerangan yang di lakukan pada 2 perangkat accsess poin, dari 2 target peneliti berhasil mendapatkan informasi password dari perangkat uji yang pertama dan untuk perangakt uji yang kedua tidak berhasil mendapatkan informasi password dari hasil percobaan penyerangan.

Tabel 3. Informasi hasil penyerangan

Jenis Serangan	Nama Perangkat	Tipe keamanan	Informasi yang Dibutuhkan	Status
Brute force Attack	TL-WR940n	WPA2/PSK	Mendapatkan informasi kemungkinan *Password*	BERHASIL
Brute force Attack	TL-WR941HP	WPA2/PSK	Mendapatkan informasi kemungkinan *Password*	GAGAL

Tabel 4. Data Log Penyerangan

Penyerangan	Jenis serangan	Target pengujian & tipe perangkat	Upaya waktu	Hasil yang didapatkan
Pengujian 1	Brute force	Yayasan, TL-WR940n	1 menit	Berhasil mendapatkan informasi *password*
Pengujian 2	Brute force	Akademik, TL-WR941HP	7 menit	Gagal mendapatkan informasi *password*

5. KESIMPULAN DAN SARAN

Berdasarkan analisis dan penjelasan yang telah diberikan sebelumnya, dapat disimpulkan dari hasil analisis keamanan jaringan *wireless* Politeknik Bhakti Asih Purwakarta dengan menggunakan metode penetration testing bahwa masih banyak celah pada hasil analisis keamanan jaringan *wireless* yaitu password yang digunakan tidak menggunakan kombinasi hufuf capital serta menggunakan simbol dalam membuat password perangkat Wi-Fi. Politeknik Bhakti Asih Purwakarta mesti meningkatkan perhatian khususnya departemen IT Politeknik Bhakti Asih Purwakarta karena setiap orang memiliki banyak peluang untuk menyerang kelemahan sistem keamanan jaringan, khususnya keamanan jaringan nirkabel. Untuk Saran penelitian selanjutnya dalam melakukan uji penetration testing terhadap perangkat wireless mesti menggunakan Operating Sistem Kalilinux, ini berlaku hanya pada Operating Kalilinux langsung tidak akan bekerja jika Operating kalilinix dijalankan pada Virtual Machine / Aplikasi Ke-Tiga yaitu Virtual Box, dan dalam pengujian mesti dilakukan kontinuitas karena brute force sendiri bekerja dengan wordlist yang dibuat oleh peneliti, jika wordlist yang dibuat secara manual akan memakan waktu yang lama maka dari itu peneliti menyarankan untuk menggunakan tools *Crunch* pada Kalilinux yang sangat membantu penguji pada pembuatan file wordlist.

DAFTAR PUSTAKA

[1] Dewa Made Julijati Putra, I Nyoman Namo Yoga Anantra, Putu Adhitya kusuma, Putu Damar Jagat Pratama, Gede Arna Jude Saskara, and I Made Edy Listartha, "Analisis Perbandingan Serangan Hydra, Medusa Dan Ncrack Pada Password Attack," *J. Inform. Teknol. dan Sains*, vol. 4, no. 4, pp. 461–466, 2022, doi: 10.51401/jinteks.v4i4.2192.

[2] Y. Mulyanto, H. Herfandi, and R. Candra Kirana, "ANALISIS KEAMANAN WIRELESS LOCAL AREA NETWORK (WLAN) TERHADAP SERANGAN BRUTE FORCE DENGAN METODE PENETRATION TESTING (Studi kasus:RS H.LMANAMBAI ABDULKADIR)," *J. Inform. Teknol. dan Sains*, vol. 4, no. 1, pp. 26–35, 2022, doi: 10.51401/jinteks.v4i1.1528.

[3] M. I. Rusdi and D. Prasti, "Penetration Testing Pada Jaringan Wifi Menggunakan Kali Linux," *Semin. Nas. Teknol. Inf. dan Komput. 2019*, pp. 260–269, 2019.

[4] I. Gunawan, "Penggunaan Brute Force Attack Dalam Penerapannya Pada Crypt8 Dan Csa-Rainbow Tool Untuk Mencari Biss," *InfoTekJar (Jurnal Nas. Inform. dan Teknol. Jaringan)*, vol. 1, no. 1, pp. 52–55, 2016, doi: 10.30743/infotekjar.v1i1.48.

[5] A. Amarudin, "Desain Keamanan Jaringan Pada Mikrotik Router OS Menggunakan Metode Port Knocking," *J. Teknoinfo*, vol. 12, no. 2, p. 72, 2018, doi: 10.33365/jti.v12i2.121.

[6] Z. Munawar, M. Kom, and N. I. Putri, "Keamanan Jaringan Komputer Pada Era Big [1] Z. Munawar, M. Kom, and N. I. Putri, 'Keamanan Jaringan Komputer Pada Era Big Data,' J. Sist. Informasi-J-SIKA, vol. 02, pp. 1–7, 2020.Data," *J. Sist. Informasi-J-SIKA*, vol. 02, pp. 1–7, 2020.

[7] Q. Qirom and M. Sungkar, "Rancang Bangun Jaringan Hotspot, Bandwidth Dan Blokir Website Berisi Konten Negatif Untuk Meningkatkan Layanan Pembelajaran Di Sd Negeri Bangun Galih 1," *Power Elektron. J. Orang Elektro*, vol. 6, no. 1, pp. 17–21, 2019, doi: 10.30591/polektro.v6i1.1188.

[8] S. Kasus, H. W. Net, A. Syaputera, and Y. Mardiana, "Hotspot Network Security System From Brute Force Attack Using Pfsense External Firewall (Case Study of Wifi-Ku . Net Hotspot) Sistem Keamanan Jaringan Hotspot Dari Serangan Brute Force Menggunakan Firewall Eksternal Pfsense," vol. 3, no. 1, pp. 205–218, 2023.

[9] Y. Mulyanto and A. A. Fari, "Analisis Keamanan Login Router Mikrotik dari Serangan Brute Force Menggunakan Metode Penetration Testing," *J. Inform. Teknol. dan Sains*, vol. 4, no. No.3, pp. 145–155, 2022.