ANALISIS KEAMANAN JARINGAN DENGAN METODE *PENETRATION TESTING EXECUTION STANDARD* (PTES) DI DINAS KESEHATAN PROVINSI JAWA BARAT

Adi Adrian[1], Angga Setiyadi[2]

[1,2] Universitas Komputer Indonesia
Jl. Dipatiukur No. 112-116, Bandung 40132
E-mail : adiadrian346@gmail.com[1], angga.setiyadi@gmail.com[2]

ABSTRAK

Penerapan jaringan kabel LAN belum menyeluruh pada setiap lantai mengakibatkan 60 persen komputer Dinas Kesehatan Provinsi Jawa Barat menggunakan jaringan *wireless.* Pada wawancara dengan Bapak Agung Aditia selaku Divisi Teknologi Informasi Komunikasi. Bahwa Dinas Kesehatan Jawa Barat sering terjadi gangguan seperti *flooding*, *illegal access*. Maka dari itu dinas kesehatan membutuhkan analisis dan audit sistem keamanan jaringan agar dapat memastikan bahwa Dinas Kesehatan Provinsi Jawa Barat baik dalam segi sistem keamanan jaringannya terutama jaringan *wireless*. Divisi Teknologi Informasi Komunikasi dalam melakukan analisis dan audit membutuhkan sebuah tools yang akan menjadi sebuah standar dalam menganalisa sistem keamanan jariangan Dinas Kesehatan Provinsi Jawa barat. Maka dari itu dibutuhkan sebuah tools standar dalam analisis dengan menggunakan *Penetration Testing Execution Standard* yang merupakan salah satu *tools* yang dikembangkan oleh *pentest organitation* untuk menjadi standar dalam menganalisis atau mengaudit sistem keamanan jaringan pada sebuah perusahaan dalam kasus ini yaitu menganalsis dan mengaudit sistem keamanan jaringan *wireless* Dinas Kesehatan Provinsi Jawa barat. Hasil dari pengujian yang telah dilakukan diantaranya, *sniffing, scanning port, scanning wireless, bruteforce*. Maka dapat disimpulkan bahwa sistem keamanan jaringan *wireless* Dinas Kesehatan Provinsi Jawa Barat masih sangat rentan terhadap serangan.

Kata Kunci : jaringan, *sniffing, scanning port, scanning wireless, bruteforce, Penetration Testing Execution Standard*

1. PENDAHULUAN

Dinas Kesehatan Provinsi Jawa Barat merupakan salah satu dinas yang berada di Provinsi Jawa Barat. Dinas Kesehatan Provinsi Jawa Barat saat ini memiliki 3 lantai, lantai 1 memiliki 4 ruangan, lantai 2 memiliki 8 ruangan, lantai 3 memiliki 4 ruangan. Masing-masing lantai memiliki 2 akses point sebagai jaringan *wireless* yang mencangkup seluruh ruangan pada setiap lantai. Penerapan jaringan kabel LAN belum menyeluruh pada setiap lantai mengakibatkan 60 persen komputer Dinas Kesehatan Provinsi Jawa Barat menggunakan jaringan *wireless.*

Jaringan *wireless* yang digunakan untuk memenuhi kebutuhan jaringan teridiri dari 6 perangkat wireless untuk mencakup seluruh lantai di Dinas Kesehatan Provinsi Jawa Barat. Perangkat *wireless* yang ada menggunakan keamanan yang berbeda diantaranya 4 perangakat terbuka (*open)* dan dua perangkat dengan jenis keamanan WPA2-PSK. Penggunaan *wireless* yang dominan ini memiliki ancaman penyerangan jaringan yang lebih rentan daripada penggunan jaringan LAN. Hal ini memaksa Divisi TIK untuk melakukan penganalisaan lebih terhadap jaringan wireless yang ada di Dinas Kesehatan Provinsi Jawa Barat.

Jaringan *wifi* memiliki lebih banyak kelemahan dibanding dengan jaringan kabel [15]. seperti pada wawancara dengan Bapak Agung Aditia selaku Divisi Teknologi Informasi Komunikasi. Bahwa Dinas Kesehatan Jawa Barat sering terjadi gangguan seperti *flooding*, *illegal access*. pada tahun yang sama pada bulan Desember, Januari, dan Februari tahun 2017 telah terjadi serangan flooding terhadap perangkat *wifi* yang berimbas pada 12 PC dan mengakibatkan keduabelas PC tersebut tidak dapat mengakses internet, serta Dinas Kesehatan Provinsi Jawa barat memiliki empat *wifi* yang terbuka dan siapapun dapat mengakses perangkat tersebut. Maka dari itu dinas kesehatan membutuhkan analisis dan audit sistem keamanan jaringan agar dapat memastikan bahwa Dinas Kesehatan Provinsi Jawa Barat baik dalam segi sistem keamanan jaringannya terutama jaringan *wireless*.

Divisi Teknologi Informasi Komunikasi dalam melakukan analisis dan audit membutuhkan sebuah tools yang akan menjadi sebuah standar dalam menganalisa sistem keamanan jariangan Dinas Kesehatan Provinsi Jawa barat. Maka dari itu dibutuhkan sebuah tools standar dalam analisis dengan menggunakan

Penetration Testing Execution Standard yang merupakan salah satu *tools* yang dikembangkan oleh *pentest organitation* untuk menjadi standar dalam menganalisis atau mengaudit sistem keamanan jaringan pada sebuah perusahaan dalam kasus ini yaitu menganalsis dan mengaudit sistem keamanan jaringan *wireless* Dinas Kesehatan Provinsi Jawa barat.

1.1 Maksud

Maksud penelitian ini untuk menganalisa sistem keamanan jaringan Dinas Kesehatan Provinsi Jawa Barat dengan menggunakan metode *penetration testing execution standard*, agar Divisi Teknologi Informasi Komunikasi mengetahui baik atau tidaknya sistem keamanan jaringan *wireless* di Dinas Kesehatan Provinsi Jawa Barat.

1.2 Tujuan

Tujuan Penelitian ini adalah untuk menginplementasikan metode *penetrarion testing execution standard* sebagai bahan analisis dan audit sistem keamanan jaringan di Dinas Kesehatan Provinsi Jawa Barat.

1.3 Metode Penelitian

Adapun Metode Penelitian yang dilakukan untuk melakukan analisis sistem keamanan jaringan *wireless* menggunakan *penetration testing execution standard* dapat dilihat pada gambar 1.



Gambar 1. *Penetration testing execution standard*

Penjelasan dari tahap-tahap metode *penetration testing execution standard* adalah sebagai berikut:

1. *Pre-engagement*

   Pre-engagement adalah tahap dimana seorang *pentester* menjelaskan kegiatan *pentest* yang akan dilakikan kepada target (perusahaan).

2. *Intelligence Gathering*

   Intelligence gathering adalah tahap dimana seorang *pentester* berusaha mengumpulkan seluruh informasi mengenai target (perusahaan) yang bisa di dapatkan dengan berbagai metode dan berbagai media. *Intelligence gathering* pada penelitian ini berfokus pada jaringan *wireless*.

3. *Threart Modeling*

   Threart Modeling merupakan pendefinisian dari pendekatan permodelan ancaman. *Threat Modeling* diperlukan untuk pelaksanaan pengujian penetrasi yang benar. Pendekatan permodelan yang dimaksud adalah pengamatan terhadap target yang bertujuan untuk mengetahui proses bisnis target agar lebih mudah dalam menentukan serangan.

4. *Vulnerability Analysis*

   Vulnerability Analysis adalah dimana tahap untuk mencari celah keamanan berdasarkan informasi yang telah didapatkan sebelumnya. *Vulnerability analysis* bertujuan untuk menemukan kekurangan didalam sistem jaringan yang dapat dimaanfaatkan oleh *pentester.*

5. *Exploitation*

   Expolition adalah tahap dimana seorangan *pentester* melakukan serangan pada target. Walaupun demikian tahap ini kebanyakan dilakukan dengan metode *brute force* tanpa memiliki unsut presisi. Seseorang *pentester* hanya akan melakukan *exploitation* ketika dia sudah mengetahui secara pasti apakah serangan yang dilakukan berhasil atau tidak, namun tentu saja ada kemungkinan tidak terduga dalam sistem keamanan target. Walaupun begitu, sebelum melakukan serangan, *pentester* harus tahu kalau target mempunyai celah keamanan yang bisa di gunakan. Melakukan serangan secara membabi-buta dan berharap sukses bukanlah metode yang produktif. Seorangan *pentester* selalu menyempurnakan analisisnya terlebih dahulu sebelum melakukan serangan yang efektif.

6. *Post-Exploitation*

   Post Exploitation adalah tahap dimana seorangan *pentester* masuk kedalam sistem jaringan target dan kemudian melakukan analisis infrastuktur yang ada. Pada tahap ini seorang *pentester* mempelajari bagian-bagian di dalam sistem dan menentukan bagian yang paling *critical* bagi target (perusahaan). Disini seorang *pentester* harus bisa menghubungkan semua bagianbagian sistem yang ada untuk menjelaskan dampak serangan atau kerugian yang paling besar yang bisa terjasi pada target (perusahaan).

7. *Reporting*

   Reporting adalah bagian paling penting dalam kegiatan *pentest.* Seorang *pentester* menggunakan *report (*laporan*)* untuk menjelaskan pada perusahaan mengenai *pentesting* yang dilakukan seperti : apa yang di lakuakan, bagaimana cara melakukannya, resiko yang bisa terjadi dan yang paling utama adalah cara untuk memperbaiki sistemnya.

2. TINJAUAN PUSTAKA

2.1 Jaringan Komputer

Jaringan komputer adalah himpunan "*interkoneksi"* antara 2 komputer *autonomous* atau lebih yang terhubung dengan media tranmisi kabel atau tanpa kabel (*wireless*). Bila sebuah komputer dapat membuat komputer lainnya restart, shutdown, atau melakukan control lainya, maka komputer-komputer tersebut bukan *autonomous* (tidak melakukan kontrol terhadap komputer lain dengan akses penuh)[1].

2.2 Tipe-tipe Jaringan Komputer

Secara umum tipe jaringan kompter dibagi menjadi dua bagian yaitu *peer to peer* dan *client server.*

1. *Peer to peer*

Peer to peer adalah tipe jaringan komputer yang memiliki sistem kerja bahwa *client* tidak dapat menjadi *server* begitu pula *server* tidak dapat menjadi *client.*

2. *Client – server*

Client -server adalah tipe jaringan komputer yang memiliki sistem kerja yaitu *client* dapat menjadi *server* serta sebaliknya *server* dapat menjadi *client.*

2.3 Jaringan LAN

Local Area Network (LAN) adalah jarigan yang di batasi oleh area yang relative kecil, umumnya dibatasi oleh area lingkungan seperti sebuah gedung perkantoran, atau sebuah sekolah, dan biasanya tidak jauh dari sekitar 1 kolometer persegi.beberapa model konfigurasi LAN biasanya berupa, satu komputer biasanya dijadikan sebuah *dile server*, yang digunakan untuk menyimpan perangkat lunak (*Software* yang mengatur aktifitas jaringan), ataupun sebagai perangkat lunak yang dapat digunakan oleh komputer-komputer yang terhubung kedalam jaringan lokal

LAN kebanyakan menggunakan media kabel untuk menghubungkan antara satu komputer dengan komputer lainnya. LAN merupakan jaringan komunikasi yang terbatas pada daerah yang kecil, misalkan sau gedung atau sekelompok bangunan kecil.[11]

2.4 Jaringan WLAN

Jaringan lokal nirkabel atau WLAN adalah suatu jaringan area lokal yang menggunakan media gelombang radio.[7]

Wireless LAN disini dapat di definisikan sebagai sistem komunikasi data fleksibel yang dapat digunakan untuk menggantikan atau menambahkan jaringan LAN yang sudah ada untuk memberikan tambahan fungsi dalam konsep jaringan komputer pada umumnya. Fungsi yang di tawarkan disini dapat berupa konektivitas yang andal sehubung dengan mobilitas *user.*[3]

Jaringan WLAN memiliki keunggulan sebagai berikut :

a. Biaya pemeliharannya murah
b. Mudah untuk di kembangkan

Jaringan WLAN pun memiliki kelemahan berupa :

a. Memiliki Delay yang besar dalam pegiriman data.
b. Seringnya signalnya terhalang.
c. Keamanan data kurang terjamin

2.5 Keamanan Jaringan

Keamanan jaringan merupakan salah satu hal penting dalam memonitoring dan mencegah penyalahgunaan sumber daya jaringan yang tidak sah dan merugikan.

a. Confidentiality

Confidentiality yaitu mensyaratkan bahwa informasi atau data hanya bisa di akses oleh pihak yang memiliki wewenang.

b. Intergrity

Intergrity yaitu , mensyaratkan bahwa informasi hanya dapat di ubah oleh pihak yang memiliki

c. *Availability*

Availability yaitu mensyaratkan bahwa informasi tersedia untuk pihak yang memiliki wewenang ketika di butuhkan

d. Authentication

Authentication yaitu Mensyaratkan bahwa pengirim suatu informasi dapat diindentifikasi dengan benar dan ada jaminan bahwa identitas yang didapat tidak palsu.

e. Nonrepudiation

Nonrepudiation yaitu Mensyaratkan bahwa baik pengirim maupun penerima informasi tidak dapat menyangkal pengiriman dan penerimaan pesan.

2.5 TCP SYN Flood *Denial of Service*

TCP SYN Flood *Denial of Service adalah* serangan *Denial of Service* dengan cara membanjiri *server* dengan *malicious request* berupa paket SYN dengan *fake source* IP *address.* SYN packet adalah paket dari client yang mengawali terbentuknya koneksi TCP/IP, setelah itu *server* akan membalas dengan SYN-ACK, dan dilengkapi engan paket SYN-ACK-ACK dari client, tiga proses ini disebut *three way handshake.* Triknya adalah pada *fake source ip address* pada paket paket SYN dari client. Akibat *server* juga tidak akan mendapatkan balasan SYN-ACK-ACK dari *client*. Padahal untuk setiap client yang mencoba membuka koneksi, server akan mengalokasikan *resource* seperti memori dan waktu untuk meunggu datangnya balsan ACK dari *client*. Dengan cara ini *attacker* menghabiskan *resource server* hanya untuk melayani *request* palsu dari *attacker*.

2.6 *Port Scanning*

Port Scanning Merupakan salah satu cara untuk mengumpulkan informasi dari target. Yang biasanya informasi yang di dapatkan berupa layanan-layanan apa saja yang disediakan, sistem operasi dan lain – lain agar dapat menentukan langkah penyerangan selanjutnya

2.7 *Brute force*

Brute Force adalah metode untuk meretas password dengan cara mencoba semua kemungkinan kombinasi yang ada pada *wordlist*. Metode *brute force* dapat dilakukan secara *online* ataupun *offline* yang menjadi kelemahan pada metode ini adalah waktu pengerjaannya yang cukup lama karna akan mencoba satu persatu *password* yang berada pada *wordlist.*

2.8 Penetration Testing Standard

Penetration Testing Execution Standart terdiri dari tujuh bagian utama. Ini mencangkup segala hal yang berkaitan dengan uji pentrasi mulai dari komunikasi awal dan penalaran di balik *pentest*, melalui fase pengumpulan informasi dan permodelan ancaman dimana penguji bekerja dibelakang layer untuk mendapatkan pemahaman yang lebih baik tentang organisasi yang di uji, melalui penelitian kerentanan, eksploitasi dan setelah eksploitasi. Seperti dapat dilihat pada gambar 2



Gambar 2. *Penetration testing execution standard*

3. ANALISIS DAN PENGUJIAN

3.1 *Pre-engagement*

Pre-engagement adalah tahap dimana seorang *pentester* menjelaskan kegiatan *pentest* yang akan dilakukan kepada perusahaan. Adapun yang dibahas pada tahap ini ini adalah pertanyaan-pertanyaan.

a. Pertanyaan *network pentration test*

Pertanyaan *network penetration test* adalah salah satu bagian dari *pre-engagement.* Pertanyaan *network penetration test* dibuat untuk membantu dalam proses wawancara agar lebih mudah dalam memberikan pertanyaan. Pertanyaan *network penetration test* dapat dilihat pada tabel 1.

Tabel 1. Pertanyaan *network pentration test*

No	Pertanyaan
1	Mengapa harus diadakanya tes penetrasi pada jaringan di Dinas Kesehatan Jawa Barat?
2	Kapan Divisi TIK menginginkan uji penetrasi keamanan ? (Saat jam kantor, Setelah jam kantor, Saat akhir pekan)
4	Berapa banyak alamat ip *internal* yang di ujikan?
5	Berapa banyak alamat ip *eksternal* yang diujikan?
6	Apakah ada perangkat terkena dampak hasil uji penetrasi, seperti (firewall, sistem deteksi, aplikasi firewall)?

b. Pertanyaan *wireless network penetration test*

Pertanyaan *wireless network penetration test* merupakan sebuah pertanyaan yang si siapkan untuk mencari informasi mengenai jaringan *wireless* target (perusahaan). Pertanyaan *network penetration test* dapat dilihat pada tabel 2.

Tabel 2. Pertanyaan *wireless network penetration test*

No	Pertanyaan
1	Seberapa Banyak Perangkat *wireless* yang aktif di Dinas Kesehatan Jawa Barat ?
2	Apakah *wireless* dapat di akses oleh orang luar, tanpa harus menggunakan hak akses ?
3	Apa jenis keamanan yang digunakan perangkat *wireless* Dinas Kesehatan Provinsi Jawa Barat ?
4	Apakah ada yang pernah mencoba menyerang melalui jaringan *wireless* Dinas Kesehatan Provinsi Jawa Barat?
5	Berapa banyak *user* yang menggunakan jaringan *wireless* di Dinas Kesehatan Jawa Barat?

c. Pertanyaan *physical penetration test*

Pertanyaan *physical penetration test* memiliki kegunaan yang sama dengan pertanyaan pertanyaan yang lainnya untuk membantu dalam pengumpulan informasi. Pertanyaan *physical penetration test* berisikan mengenai cangkupan penelitian. Pertanyaan *physical penetration test* dapat dilihat pada tabel 3.

Tabel 3. Pertanyaan *physical penetration test*

No	Pertanyaan
1	Berapa Lantai yang akan menjadi cangkupan pengujian?
2	Lantai mana saja yang masuk dalam cangkupan pengujian ?
3	Apakah Dinas Kesehatan Provinsi Jawa Barat memiliki *standard operating procedure* (S.O.P) dalam akses, perawatan, dan penanganan jaringan ?
4	Apakah ada berita acara atau dokumentasi tentang keamanan jaringan ?
5	Apakah terdapat kamera *cctv* di Dinas Kesehatan Provinsi Jawa Barat ?

d. Pertanyaan *administrator* sistem

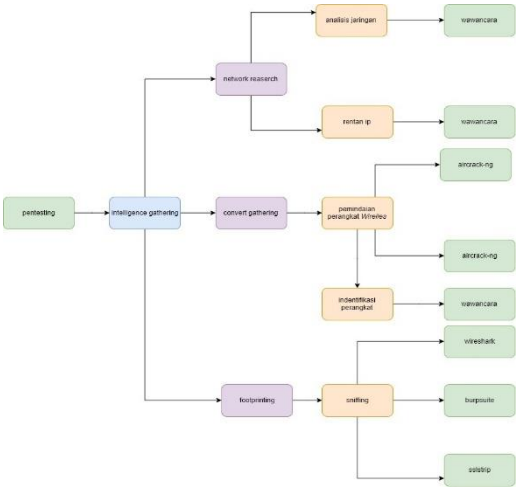
Pertanyaan administrator sistem adalah pertanyaan yang berisikan mengenai pertanyaan yang ditujukan untuk mengetahui tentang *administrator* sistem yang ada pada target. Pertanyaan *administrator* sistem dapat dilihat pada tabel 4.

Tabel 4. Pertanyaan *administator* sistem

No	Pertanyaan
1	Apakah sistem operasi selalu *update?*
2	Apakah ada perangkat lunak pemantauan sistem?
3	Apakah *Backup* data *server* dilakukan secara teratur ?
4	Kapan terkhir *Restore Backup* data *server* ?

3.2 *intelligence gathering*

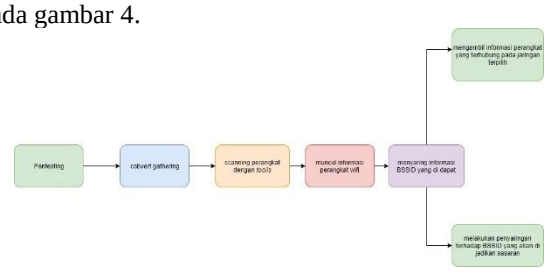
Interlligence Gathering adalah tahap dimana seorang *pentester* berusaha mengumpulkan sebanyak mungkin informasi mengenai perusahaan target yang bisa didapatkan dengan berbagai metode dan berbagai media. Adapun alur yang dimiliki oleh *intelligence gathering* dapat dilihat pada gambar 3.



Gambar 3. Alur *intelligence gathering*

a. Convert Gatehring

Covert Gathering atau pengintaian merupakan kegiatan yang ada pada metode *penetration testing execution standard*. pengintaian bertujuan untuk mengetahui target (perushaan). Berikut adalah alur dari *convert gathering* dapat dilihat pada gambar 4.



Gambar 4. Alur *convert gathering*

b. Footprinting

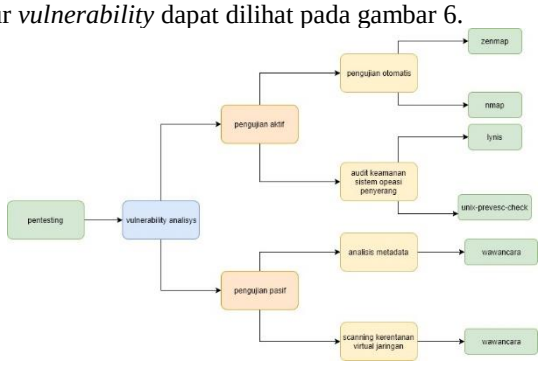
Footpriting adalah fase pengumpulan informasi yang terdiri dari interaksi dengan target untuk mendapatkan informasi dengan cara menguji target. Pengujian *footpinting* dilakukan dalam *footprinting internal*. *Footprinting* memiliki alur yang dapat dilihat pada gambar 5.



Gambar 5. Alur *footprinting*

3.2 *Vulnerability Analisys*

Vulnerability Analisis adalah dimana tahap untuk mencari celah keamanan berdasarkan informasi yang telah didapatkan sebelumnya. *Vulnerability analisis* bertujuan untuk menemukan kekurangan didalam sistem jaringan yang dapat dimanfaatkan oleh penyerang. Adapun alur *vulnerability* dapat dilihat pada gambar 6.

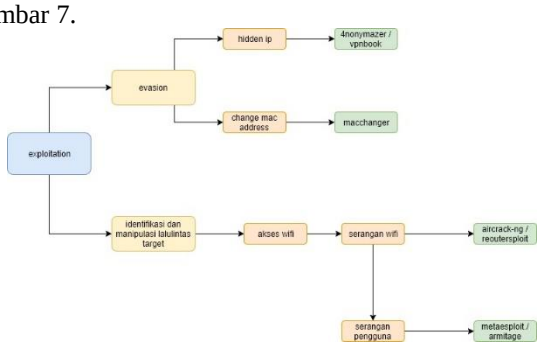


Gambar 6. Alur *vulnerability analisis*

4. Implementasi dan Pembahasan

4.1 *Explotation*

Exploitation adalah tahap dimana *pentester* memanpaatkan celah yang didapatkan dari hasil pencarian informasi sebelumnya. Dengan kata lain exploitation adalah penyerangan terhadap target setelah mendapatkan informasi dari target. Adapun alur exploitation dapat dilihat pada gambar 7.



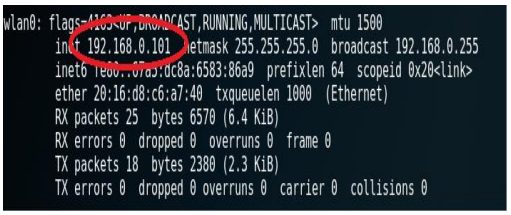
Gambar 7. Alur *exploitation*

a. *Evasion*

Dalam melakukan penetrasi sebaiknya *pentester* selalu menyembunyikan identitas saat melakukan percobaan untuk menghindari pendeteksian yang dilakukan oleh sistem. maka *evasion* merupakan sebuah teknik untuk menghindari kemungkinan terdeteksi serangan.

1. **Merubah *Ipaddress pentester* dengan *tools vpn books***

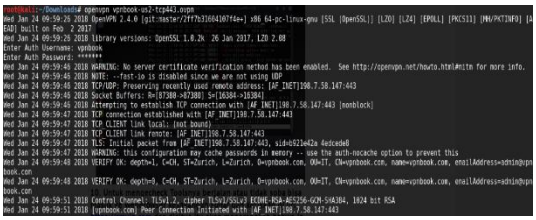
Ip address yang digunakan oleh *pentester* adalah 192.168.0.101. Berikut ini adalah gambar penggilan informasi *interface pentester*. Dapat dilihat pada gambar 8.



Gambar 8. Tampilan *ifconfig*

2. **Meng*install vpnbook***

Langkah untuk menginstall vpnbook dengan menuliskan perintah "*openvpn vpnbook -us2-tcp443.ovpn"* pada terminal *linux* Berikut adalah tampilan dari menginstall vpnbook dapat dilihat pada gambar 9.



Gambar 9. Menginstall vpnbook

3. **Pembuktian *ipaddress* telah dirubah**

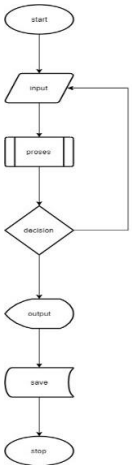
Untuk membuktikan bahwa ipaddress telah berhasil dirubah maka dibuktikan dengan mengecek ip dan region dengan situs *https://cmyip.com* berikut adalah tampilan ip yan telah dirubah dapat dilihat pada gambar 10.



Gambar 10. Pembuktian perubahan *ipaddress*

b. *Brute force*

Brute force adalah teknik untuk melakukan login dengan mencoba segala kemungkinan dan kominasi dari username dan passowrd hingga ditemukan kombinasi yang benar. Adapun alur pada *brute force* dapat dilihat pada gambar 11.



Gambar 11. Alur *brute force*

1. Mengaktifkan mode montoring interface wlan0
   Untuk menggunakan *tools* aircrack-ng diperlukan untuk mengaktifkan mode monitoring pada *interface wlan0* menggunakan perintah " *airmon-ng start wlan0".* Berikut adalah tampilan dari mode monitoring dapat dilihat pada gambar 12.



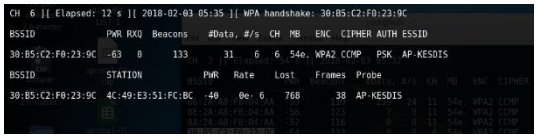
Gambar 12. mode monitoring interface wlan0

2. Perintah *airodump-ng* wlan0mon pada console digunakan untuk *scanning wireless.* Berikut ini adalah layar keluaran hasil dari mengetikan perintah *airodump-ng wlan0mon* dapat dilihat pada gambar 13.



Gambar 13. Tampilan hasil dari perintah *airodump-ng wlan0mon*

3. Perintah *airodump-ng –bssid C4:6E:IF:D8:B1 -c 6 -w /root/Dekstop/ujicoba2 wlan0mon* digunakan untuk menghubungkan atau *handshake interface pentester* dengan perangkat *wireless* target. Berikut adalah tampilan dari *handshake* perangkat. Dapat dilihat pada gambar 14.



Gambar 14. Handshake perangkat *wireless*

4. Perintah *aircrack-ng /root/Dekstop/ujicoba02-01.cap -w /root/Dekstop/WD.lst di gunakan untuk* meng*load* file .lst dan menjalan *tools aircrack-ng* untuk melakukan *bruteforce* pada perangkat *wireless* target. Berikut adalah tampilan dari aircrack dapat dilihat pada gambar 15.



Gambar 15. Tampilan aircrack

4.2 Pelaporan

Pelaporan dibuat setelah kegiatan *penetration testing* selesai dilakukan. Laporan berisi tentang hasil dan pembahasan dari setiap tahapan yang disebutkan pada laporan *penetration testing* dapat dijadikan dasar untuk pemberian saran dalam penelitian ini.

5. Kesimpulan

Berdasarkan hasil dari uraian *pentest* di Dinas Kesehatan Provinsi Jawa Barat memiliki banyak celah yang harus lebih diperhatikan oleh Divisi Teknologi Informasi Komunikasi Dinas Kesehatan Provinsi Jawa Barat karena banyak sekali kesempatan bagi siapapun untuk menyerang kelemahan sistem keamanan jaringan terutama keamanan jaringan *wireless.*

DAFTAR PUSTAKA

[1] M. Syafrizal, pengantar jaringan komputer, Yogyakarta: Penerbit Andi, 2005.

[2] Admin, "Sejarah," 05 Juni 2014. [Online]. Available: http://www.diskes.jabarprov.go.id/index.php/pages/detail/2014/6. [Accessed 4 Maret 2017].

[3] A. Satria, "PENGEMBANGAN PERANGKAT WIRELESS IDS(INTRUSION DETECTION SYSTEM) BERBASIS EMBEDDED SYSTEM (STUDI KASUS : BADAN NARKOTIKA NASIONAL)," 2011.

[4] A. A. ,. E. Randy Mentang, "PERANCANGAN DAN ANALISIS KEAMANAN JARINGAN NIRKABEL MENGGUNAKAN WIRELESS INTRUSION DETECTION SYSTEM," vol. 5, 2015.

[5] Kairulanam, "SISTEM PENDETEKSI SERANGAN PADA JARINGAN KOMPUTER MENGGUNAKAN SNORT BERBASIS SMS GATEWAY (STUDI KASUS DI TAMAN PINTAR YOGYAKARTA)," 2011.

[6] S. Surianto Rustan, mendisain logo, jakarta: Gramedia Pustaka utama, 2009.

[7] W. Komputer, SPP MENGINSTALASI PERANGKAT JARINGAN KOMPUTER, JAKARTA: PT Elex Media Komputindo, 2006.

[8] D. Ariyus, PENGANTAR ILMU KRIPTOGRAFI Teori, Analisis, dan Implementasi, Yogyakarta: ANDI OFFSET, 2008.

[9] M. D. S. M. T. A. S. Agung baitul Hikmah, CARA CEPAT MEMBANGUN WEBSITE DARI NOL STUDI KASUS WEB DEALER MOTOR, Yogyakarta: Andi OFFSET, 2015.

[10] T. A. Prabawati, TUTORIAL 5 HARI : BELAJAR HACKING DARI NOL, Yogyakarta: CV. ANDI OFFSET, 2010.

[11] B. Irawan, JARINGAN KOMPUTER, YOGYAKARTA: GRAHA ILMU, 2005.

[12] M. Dony Ariyus, INTRUSION DETECTION SYSTEM sistem pendeteksi penyusup pada jaringan komputer, Yogyakarta: CV.ANDI OFFSET, 2007.

[13] H. Alffata, ANALIS & PERANCANGAN SISTEM INFORMASI untuk keunggulan bersaing perusahaan & organisasi modren, Yogyakarta: CV.ANDI OFFSET, 2007.

[14] Z. A. Ricardo Luis Daloca, "NOVEL ALGORITHMS AND TECHNIQUES IN TELECOMMUNICATIONS AND NETWORKING," *an architecture for wireless intrusion detection system using artificial neural networks*, p. 357, 2010.

[15] A. A. A. D. Batara Sakti, "Uji Kelayakan Impletasi SSH sebagai pengaman FTP Server dengan Penetration testing," vol. 2, no. 1, pp. 1- 8, 2013.

[16] A. Setiyadi, "Implementasi MITM pada Websploit sebagai Monitoring Aktifitas pengguna dalam Mengakses Internet," pp. 1-8, 2017.