EVALUASI PENERAPAN AUTENTIKASI PENGGUNA WIRELESS LAN BERBASIS RADIUS SERVER UNIVERSITAS BINA DARMA

Abdul Aziz Ar
Mahasiswa Universitas Bina Darma
Jln. A. Yani No. 12 Palembang, Sumatera Selatan, Indonesia
Pos-el: abdoelazizar@gmail.com

Abstract: *RADIUS (Remote Access Dial in User) is a widely used protocol for authentication of network users . Simply stated , provides RADIUS authentication function , authorization and accounting or known as AAA (Authentication , Authorization and Accounting) to use network services . RADIUS technology developments that are currently growing cause a lot of positive and negative impacts that now implemented at Bina Darma University Palembang . When this technology used in a long time and the number of users who access increases. The purpose of this study is to see the security of the RADIUS server , as seen from the software used and the penetration test against a RADIUS server . With the action research method , to evaluate the results of the implementation of the RADIUS server and be considered a network administrator . the author intends to write a research entitled " Evaluation of Wireless LAN -Based Authentication RADIUS Server Case Study of Bina Darma University " .*
Keyword : Radius, Autentikasi, Effective, Security, Action Research

Abstrak: *RADIUS (Remote Access Dial in User)* merupakan suatu protokol yang digunakan secara luas untuk autentikasi pengguna jaringan. Secara sederhana, *RADIUS* menyediakan fungsi autentikasi, otorisasi dan akunting atau lebih dikenal dengan *AAA (Authentication, Authorization dan Accounting)* untuk menggunakan layanan jaringan. Perkembangan teknologi RADIUS yang saat ini berkembang menimbulkan banyak dampak positif dan negatif yang sekarang diimplementasikan di Universitas Bina Darma Palembang. Ketika teknologi ini digunakan dalam waktu yang lama dan dengan jumlah penguna yang mengakses semakin bertambah. Tujuan dari penelitian ini adalah untuk melihat security dari *RADIUS server*, yang dilihat dari *software* yang digunakan dan dengan test penetrasi terhadap *RADIUS server*. Dengan metode *action research*, untuk mengevaluasi hasil dari implementasi dari *RADIUS server* dan menjadi bahan pertimbangan seorang *administrator* jaringan. maka penulis berkeinginan untuk menulis penelitian dengan judul "Evaluasi Autentikasi *Wireless LAN* Berbasis *Radius Server* Studi Kasus Universitas Bina Darma".
Kata kunci : *Radius, Autentikasi, Effective, Security, Action Research*

1. PENDAHULUAN

Teknologi Informasi dan Komunikasi sudah banyak membawa dampak positif dalam kebutuhan akan informasi dan komunkasi. Dampak yang sangat di rasakan di dalam telekomunikasi adalah penggunaan teknologi *Wireless LAN*. Dengan menggunakan teknologi *Wireless LAN* suatu informasi yang dulu diakses dengan menggunakan kabel dan *modem* saat ini sudah bisa digantikan dengan teknologi *Wireless LAN* yang dapat kita temui di sekolah – sekolah, perkantoran - perkantoran, rumah sakit dan beberapa tempat umum. Dengan kemudahan ini, semua informasi bisa didapatkan hanya dalam waktu hitungan menit.

Sutjipta (2009) mengatakan bahwa evaluasi adalah penilaian secara sistemik untuk menentukan atau menilai kegunaan, keefektifan sesuatu yang didasarkan pada kriteria tertentu dari program.

Universitas Bina Darma telah menerapkan jaringan *Wireless LAN* RADIUS *(Remote Authentication Dial-In User)* sejak 30 Juli 2010 sebagai sistem keamanan jaringan *Wireless LAN* yang terdapat pada seluruh kampus Universitas Bina

Darma. Belum adanya evaluasi secara sistemik terhadap autentikasi layanan *HOTSPOTUBD*, maka diperlukan evaluasi terhadap autentikasi agar dapat mengetahui tingkat keamanan jaringan *HOTSPOTUBD.*

Imam Cartealy (2013) mengatakan bahwa *RADIUS (Remote Access Dial in User)* merupakan suatu protokol yang digunakan secara luas untuk otentikasi pengguna jaringan. Secara sederhana, *RADIUS* menyediakan fungsi otentikasi, otorisasi dan akunting atau lebih dikenal dengan *AAA* (*authentication, authorization* dan *accounting)* untuk menggunakan layanan jaringan.

Pengguna yang terhubung dengan *HOTSPOTUBD* di Universitas Bina Darma dari tahun ke tahun semakin bertambah. Hal ini dilihat dari jumlah mahasiswa yang mendaftar setiap tahunnya. Selain mahasiswa, dosen dan karyawan juga dapat mengakes jaringan dengan menggunakan nama pengguna dan kata kunci yang berbeda. *Wireless LAN RADIUS server* yang ada di Bina Darma adalah jaringan yang bebas *(public)*, kemungkinan untuk diretas sangat tinggi oleh pengguna yang tidak punya hak akses terhadap jaringan.

Salah satu aspek dalam mengontrol akses sebuah *user* menurut J.Hassel, (2002), yaitu Autentikasi *(Authentication);* yaitu proses pengesahan identitas pengguna *(end user)* untuk mengakses jaringan. Proses ini diawali dengan pengiriman kode unik misalnya, *username, password, pin*, sidik jari oleh pengguna kepada *server*. Di sisi *server,* sistem akan menerima kode unik tersebut, selanjutnya membandingkan dengan kode unik yang disimpan dalam *database server*. Jika hasilnya sama, maka *server* akan mengirimkan hak akses kepada pengguna. Namun jika hasilnya tidak sama, maka *server* akan mengirimkan pesan kegagalan dan menolak hak akses pengguna.

Penelitian ini bertujuan untuk mengevaluasi autentikasi *HOTSPOTUBD* yang telah diterapkan di Univeristas Bina Darma, untuk mengetahui keamanan, dalam menunjang kemajuan teknologi dan informasi yang ada di Universitas Bina Darma, yang nantinya akan memberikan masukan dalam proses pengembangan *Wireless LAN RADIUS server* kedepan.

2. METODOLOGI PENELITIAN

2.1. Metode Penelitian

Adapun metode penelitian yang digunakan dalam penelitian ini adalah menggunakan metode tindakan *(action research).* Menurut Gunawan (2007), *action research* adalah kegiatan dan atau tindakan perbaikan sesuatu yang perencanaan, pelaksanaan, dan evaluasinya digarap secara sistematik dan sistematik sehingga validitas dan reliabilitasnya mencapai tingkatan riset.

Tahapan-tahapan action research berikut:

1. Melakukan Diagnosa (*Diagnosing*) pada tahapan ini peneliti akan melakukan identifikasi masalah – masalah yaitu bagaimana cara mengevaluasi penerapan autentikasi *HOTSPOTUBD* berbasis *RADIUS server.*
2. Membuat Rencana Tindakan *(Action Planning)* tahapan ini peneliti melakukan pemahaman pokok masalah yang ada dan menyusun rencana tindakan yang tepat untuk menyelesaikan

masalah yang ada. Peneliti akan mulai menyusun rancangan untuk deskripsikan pemanfaatan *HOTSPOTUBD* yang ada di Universitas Bina Darma.

3. Melakukan Tindakan *(Action Taking)* mengimplementasikan rencana tindakan yang telah disusun, dengan mulai melakukan tahapan - tahanap analisa, evaluasi, menginvestigasi dan pengujian guna mendapatkan informasi kekurangan *HOTSPOTUBD* Universitas Bina Darma.
4. Melakukan Evaluasi *(Evaluating)* setelah tahapan *Action Taking* sudah dilakukan penulis mulai melakukan evaluasi pada hasil dari implementasi sebelumnya dan mulai menyimpulkan hasil dari langkah sebelumnya.
5. Pembelajaran *(Learning)* langkah ini merupakan tahap akhir dari penelitian yaitu melakukan *review* terhadap hasil dari tahapan-tahapan yang telah dilalui.

2.2. Metode Pengumpulan Data

Dalam pengumpulan data untuk penelitian evaluasi autentikasi *HOTSPOTUBD* berbasis *radius server*, digunakan beberapa cara, yaitu:

1. *Observasi* dilakukan peninjauan langsung di kampus utama, Universitas Bina Darma, observasi juga dilakukan ke bagian unit pelaksanaaan teknis (UPT-SIM).
2. Wawancara dengan melakukan tanya jawab langsung dengan mahasiswa dan dosen yang cendrung sering mengakses *Wireless LAN*.
3. Studi Pustaka, mempelajari, mencari dan mengumpulkan data yang berhubungan dengan penelitian seperti buku dan *internet* yang berkaitan tentang evaluasi *wireless* LAN yang berbasis *RADIUS server*.

2.3. Metode Testing

Metode testing yang digunakan dalam penelitian ini adalah metode test penetrasi *(Penetration Test)*. *Penetration testing* merupakan tindakan yang membahayakan data (Whitaker, 2005) karena pelaku pengujian bersifat aktif dalam melakukan berbagai serangan untuk mencari kelemahan sistem. Penerapan *penetration testing* pada sebuah institusi membutuhkan perencanaan dan persiapan yang matang sehingga tidak beresiko besar yang bersifat merugikan pihak institusi selaku pemilik aset dan pihak pelaku pengujian. Metodologi yang digunakan untuk melakukan *penetration testing* untuk WLAN sudah ada seperti yang dikeluarkan oleh lembaga OIISG *(Open Information System Security Group)* yang terdokumentasi dalam ISSAF *Penetration testing*. ISSAF *(Information Systems Security Assessment Framework)* merupakan kerangka kerja yang dapat digunakan sebagai acuan untuk melakukan assessment keamanan sistem.

3. HASIL

3.1. Scanning

Peneliti memanfaatkan *tools airodum-ng* untuk mendapatkan informasi tentang *HOTSPOTUBD,*

Tabel 3.1. Daftar *HOTSPOTUBD* kampus Utama Universitas Bina Darma

BSSID	CH	MB	ESSID
C0:C1:C0:09:FB:9E	*6*	54e	*HOTSPOTUBD* Utama Lantai Dasar
68:7F:74:54:75:AE	6	11	*HOTSPOTUBD* Lantai 2
68:7F:74:54:73:DA	6	54e	*HOTSPOTUBD* Lt. 2 RUANG DOSEN
68:7F:74:54:75:9C	8	54	*HOTSPOTUBD* Utama

3.1.1. *Scanning hotspotUDB* dengan Nikto

Nikto adalah *tools* untuk pemeriksaan *vulnerability* pada *apache*. Hasil dari *scanning* bisa dilihat pada gambar 3.1.

Gambar 3.1. *Scanning* Nikto

Dari hasil *scanning* dapat dilihat bahwa: *Vulnerable applications version* adalah *Apache/2.2.12 appears to be outdated (current is at least Apache/2.2.22). Apache 1.3.42 (final release) and 2.0.64 are also current.*

Dari *vulnerable applications version* dilihat bahwa ada satu *server apache* yang harus di *update* ke versi yang terbaru, agar kelemahan – kelemahan yang diakibatkan kadaluawarsa tertutup.

Vulnerable sensitive data exposure:

a. *OSVDB-3092: /phpmyadmin/changelog.php: phpmyAdmin is for managing MYSQL databases, and should be protected or limited to authorized hosts.*
b. *OSVDB-3268: /icons/: Directory indexing found.*
c. *OSVDB-3233: /icons/README: Apache default file found.*

3.1.2. *Scanning HOTSPOTUBD* Dengan OpenVAS

OpenVAS merupakan bagian dari *vulnerability Analysis* yang terdapat pada *operating system kali linux*, dengan mengakses dari *localhost* atau menggunakan alamat 127.0.0.1:9392 pada *address bar browser*. Dengan *user* dan *password* yang sudah didapat pada saat OpenVas-setup.

Gambar. 3.2. *Report scanning* OpenVAS

Berdasarkan *Security Issues for Host HOTSPOTUBD* dari hasil *scanning* dengan menggunakan OpenVAS di ketahui ada 4 *vulnerable* yang berbahaya:

1. Apache httpd *Web Server* Range Header Denial of Service Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.901203) pada port 80

2. Multiple IP Video/Camera *Server Web* Interface Default Admin Credentials (OID: 1.3.6.1.4.1.25623.1.0.103887) pada port 80

3. Apache httpd *Web Server* Range Header Denial of Service Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.901203) pada port 443.

4. Multiple IP Video/Camera *Server Web* Interface Default Admin Credentials (OID: 1.3.6.1.4.1.25623.1.0.103887) pada port 443.

3.1.3. *Scanning HOTSPOTUBD* dengan Nessus

Dari hasil *scanning* menggunakan nessus di ketahui ada 2 *vulnerable* yaitu informasi tentang port port yang terbuka pada ip 10.237.15.222.

Adapun dua *vulnerable* yang merupakan informasi adalah:

1. *Nessus SYN scanner*, ini adalah *plugin SYN* setengah terbuka atau *'half-open'* pada *firewall*. *SYN scanner* kurang *intrusif* dari *TCP (full connect) scanner* terhadap *SYN* menyebabkan layanan terganggu, hal ini menyebabkan masalah untuk *firewall* dikarenakan *firewall* yang kurang kokoh dan meninggalkan koneksi tertutup pada target jarak jauh, jika jaringan dimuat. Solusinya adalah Lindungi target Anda dengan filter IP.
2. *Ping the remote host*, *Plugin* ini mencoba untuk menentukan apakah *host remote* hidup menggunakan satu atau lebih, jenis *ping:*

a. *Ping* ARP, disediakan tuan rumah adalah pada subnet lokal dan Nessus adalah berjalan di atas ethernet.
b. *Ping* ICMP.
c. *Ping* TCP, di mana plugin mengirimkan ke host remote paket dengan flag SYN, dan tuan rumah akan membalas dengan RST atau SYN / ACK. UDP *ping* (DNS, RPC, NTP, dll).

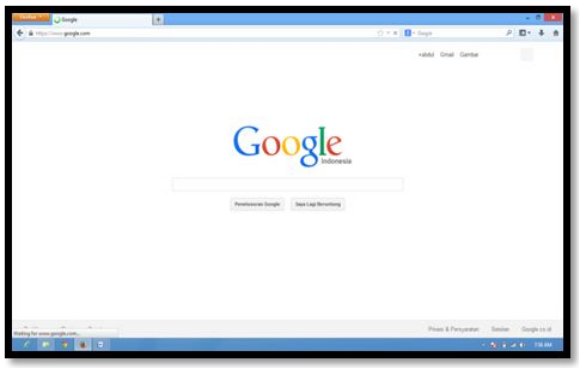
3.1.4. *Scanning* dengan Acunetix

Acunetix adalah *software scanning* yang sering digunakan oleh para *attacker* untuk menemukan celah celah keamanan dari target. Peneliti menggunakan acunetix untuk melihat celah keamanan dari portal autentikasi *HOTSPOTUBD*.

3.2. *Exploit / Attack*

3.2.1. DoS

Tujuan dari *attacking* menggunakan DoS adalah untuk menguji server dan perangkat lainnya dengan menggunakan teknik dos apakah jaringan HOTSPOTUBD mempunyai teknik untuk menahan jumlah paket dalam jumlah yang besar.



Gambar 3.3. Tampilan Awal Sebelum Dilakukan DoS.

1. Mdk3

Penliti menggunakan mdk3 untuk melakukan DOS dengan target pengujian *HOTSPOTUBD* Utama, essid 68:7F:74::54:75:9C, *channel* 8 yang ada di kampus utama lantai 4,

Mdk3 berasil membuat jaringan *HOTSPOTUBD* terganggu selama proses dos berlangsung *user* tidak dapat melakukan koneksi. Untuk mengembalikan jaringan keposisi awal pada terminal yang sedang

menjalankan mdk3 tinggal menekan ctrl + c, maka jaringan membutuhkan waktu kurang dari 1 menit.

2. Airplay-ng

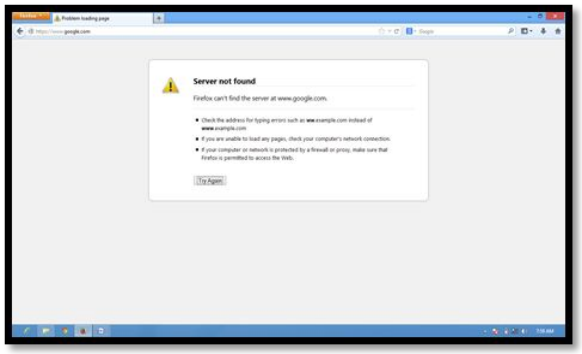
Selain menggunakan Mdk3 peneliti juga menggunakan *airplay-ng* untuk melakukan DOS ke jaringan *HOTSPOTUBD*. Dengan menggunakan BSSID *HOTSPOTUBD* Utama, ESSID 68:7F:74::54:75:9C dan channel 8.

Sama seperti mdk3 *airplay-ng* berasil melumpuhkan *server*, *user* yang terhubung secara otomatis akan terputus, dilihat dari jumlah paket yang diterima oleh *server HOTSPOTUBD* cukup untuk memutuskan semua akses jaringan dengan cepat.

3. ***Low Orbit Ion Cannon* (LOIC)**

LOIC adalah *software* DoS yang compatible di windows, LOIC dapat digunakan oleh satu komputer attack dan akan lebih baik digunakan dalam jumlah beberapa kompuer, sehingga downtime akan lebih banyak.

Dari beberapa pengujian dengan beberapa *tools* DoS, *HOTSPOTUBD* perlu dilakukan konfigurasi *firewall* agar kerentangan terhadap DoS dapat dibatasi, sehingga *server* tidak terbebani oleh paket yang dikirim *attacker*.



Gambar 3.4. Tampilan Browser *Client* Sesudah DoS dengan Menggunakan Mdk3, *Airplay-ng* dan Loic.

3.2.2. *Session Hijacking*

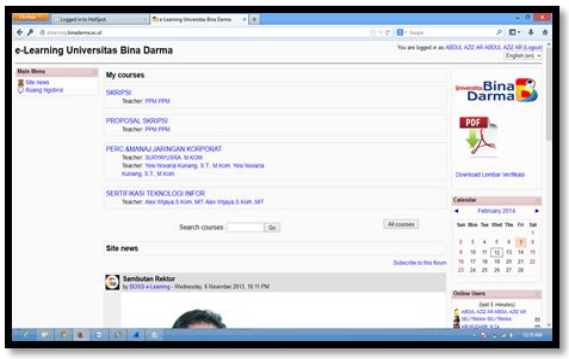
1. Airodump-ng

Untuk mendapatkan session hijacking peneliti menggunakan tools airodump-ng. Dari pengujian dengan menggunakan tools airodump-ng peneliti tidak dapat mendapatkan akses ke dalam *HOTSPOTUBD*, hal ini dikarenakan jumlah paket yang ada kurang banyak. Pergantian MAC berasil dilakukan tapi hal ini tidak mendapat respon terhadap jaringan *HOTSPOTUBD*.

***2. Cookies* manager (Mozila firefox)**

Cookies manager adalah fasilitas yang ada pada *add ons* yang dapat di *install* pada browser untuk kepentingan *development*, penulis memanfaatkan *browser* untuk melakukan pergantian *cookies* dari pengguna lainya dengan memanfaatkan wireshark.

Wireshark merupakan *tools* yang paling sering digunakan untuk melakukan *capture* paket, selain itu wireshark juga *support* digunakan di *operating system* windows dan Linux.



Gambar 3.5. *Cookies* Berasil di duplikasi.

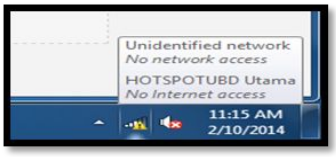
Berdasarkan penelitian yang dilakukan, diketahui *cookies* yang didapat pada paket pcap. Jika sudah lama disimpan tidak dapat digunakan, tapi *cookies* yang baru didapat bisa digunakan.

3.2.3. *Disconnected Computer Client*

1. Tuxcut

Tuxcut adalah aplikasi berbasis Linux yang digunakan untuk me*monitoring client* yang terhubung dalam satu jaringan yang sama dengan memanfaatkan IP dari target. Tuxcut digunakan sebagai alat memutuskan *client* yang terhubung dengan berbagai tujuan. Peneliti menggunakan tuxcut dengan tujuan untuk membuktikan apakah HOTSPOTUBD dapat melindungi *client* yang sedang menggunakan jaringan wirelessnya.

Setelah dilakukan *cutting* jaringan terhadap IP 192.168.18.24, *client* yang terhubung ke jaringan *HOTSPOTUBD* tidak mendapatkan akses ke jaringan lagi. Sampai *attacker* melakukan remove pada ip yang di cutnya.



Gambar 3.6. Terputusnya Jaringan Target

2. Netcut

Tidak menutup kemungkinan bahwa *user* yang menggunakan sistem operasi Windows tidak bisa melakukan hal yang sama dengan para *attacker* yang menggunakan sistem operasi linux. Fasilitas *Disconnected Computer Client* yang ada di windows diantaranya netcut prinsip kerja hampir sama dengan menggunakan tuxcut, *attacker* mendapatkan akses untuk memutuskan jaringan target yang terhubung dengan menggunakan ip seperti gambar dibawah ini dan melakukan *cutting* ke ip target.

3.2.4. Sniffing

1. Menggunakan Hamster

Pada pengujian pertama peneliti gagal untuk mendapatkan *cookies* dari target dengan manfaatkan wireshark, peneliti menggunakan hamster 2.0, untuk mendapatkan *cookies* dari *client* yang melakukan login ke *web site*. Hamster berjalan di *operating system* kali linux dan diakses secara *localhost* pada *browser* yang sudah dilakukan *setting proxy* 127.0.0.1:1234.

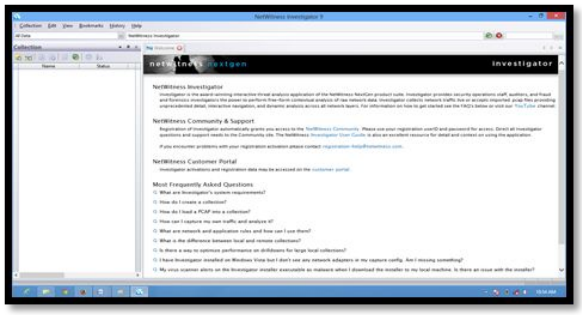
Gambar 3.7. Hamster 2.0

Hamster me*monitoring* kegiatan dari *client* yang terhubung dalam satu jaringan yang sama memanfaatkan session dari *client attacker* menunggu target melakukan login ke *web site*, target utama adalah akun yang digunakan target untuk login. Hasil dari sniffing menggunakan hamster tidak dapat dilakukan Karena target terhiden atau tidak dapat dikenali.

2. Menggunakan Netwitness

Netwitness adalah *software forensic* yang digunakan untuk *investigator* menganalisa paket pcap. Peneliti penggunakan Netwitness untuk

memantau kegiatan *client* berdasarkan paket yang di terima dari wireshark.



Gambar 3.8. Netwitness

Gambar 3.9. Paket yang berhasil di *import* dari *Netwitness*

Dari hasil penelitian dengan menggunakan netwitness dapat dilihat beberapa *url* yang dikunungi oleh *client* yang terhubung dengan HOTSPOTUBD, selain itu informasi tentang pengguna dapat dilihat, seperti *user id*dan *password* yang digunakan.

Gambar 3.10. *Query* dari *User id* dan *Password* ditemukan

3.3. Melakukan Evaluasi *(Evaluating)*

Setelah dilakukan observasi dan wawancara langsung di Universitas Bina Darma, hasil *information gathering* ditemukan beberapa temuan diantaranya;

1. Jaringan *wireless* Hotspot UBD merupakan jaringan yang sistem keamanannya menggunakan RADIUS sebagai *autentikasi* antara server dengan *client*. Dimana radius menjalankan sistem administrasi pengguna yang terpusat, dan sistem ini akan mempermudah tugas administrator.
2. *System authentication user* dan *password* yang atur secara *default user id*dan *password* sama, seharusnya dibuat berbeda antara *user id*dan *password* hal ini membuat sistem yang terkoneksi ke *database* lainya dengan mudah dimasuki *attacker*.
3. *Password* expiration atau panjang *password* minimum dan perpaduan capital, symbol dan angka, merupakan hal yang sangat penting untuk menjamin keaman *user*. Ini berdampak buruk bagi beberpa *user* baru “mahasiswa semester satu” yang tidak mengerti akan pentingnya *user id*dan *password*.
4. Belum adanya fasilitas lupa *password* yang disingkronisasikan dengan email. Jadi *user* tidak perlu melakukan konfirmasi keadmin langsung, dengan menggunakan *email user* dapat mengganti dan membuat *password* baru.
5. Belum adanya sistem pemblokiran terhadap user yang melakukan login secara terus menerus dengan *user id*dan *password* yang salah.

3.3.1. Evaluasi Hasil *Attacker*

Dari hasil penetrasi dengan menggunakan berbagai teknik pentrasi didapatkan temuan – temuan yang dapat di jadikan pembelajaran agar dapat di lakukan analisa dan evaluasi lebih lanjut diantaranya;

1. *DoS (Deniel of Service)* peneliti berasil melakukan teknik ini dengan membanjiri server menggunakan paket – paket memanfaatkan aplikasi MDK3, Airplay-ng dan LIOC. Server *HOTSPOTUBD* tidak dapat diakses oleh *attacker* dan *client* lainya pada saat melakukan DoS jumlah paket yang dikirim rata – rata sebanyak 1000 paket.
2. *Session hijacking* menggunakan airodump-ng tidak dapat dilakukan, peneliti berasil mendapatkan MAC dari target dan mengganti dengan MAC didapat, hal ini membuat jaringan penelti tidak dapat akses internet HOTSPOTUBD. Selain menggunakan airodump-ng, peneliti menggunakan *cookies* manager untuk mendapatkan akses *user id*dan *password* dari target.
3. *Disconnected computer client*, menggunakan tuxcut dan netcat berasil dilakukan *client* yang menjadi target dapat putuskan akses internetnya. Hasil dari tuxcut dan netcat mengurangi jumlah *client* hal ini berdampak buruk bagi user yang sedang menggunakan jaringan HOTSPOTUBD.
4. *Sniffing*, dari hasil *monitoring* terhadap jaringan HOTSPOTUBD menggunakan hamster tidak mendapatkan hasil, target tidak dapat ditemukan. Selain menggunakan hamster peneliti menggunakan netwitness, dengan memanfaatkan paket yang dicapture oleh wireshark, peneliti dapat me*monitoring* kegiatan *client* yang terhubung kejaringan dan mendapatkan *user id*dan *password* dari user yang melakukan login ke *web site* yang menggunakan http.

3.4. Pembelajaran *(Learning)*

3.4.1. Dokumentasi dan Pelaporan (*Documentation and Reporting*)

Dokumentasi dan pelaporan hasil pengujian dengan menggunakan metode pengujian penetration testing.

1. *Deniel of Service* dengan Melakukan serangan dengan mengirimkan paket TCP, UDH, HTTP sehingga *server* menerima paket dalam jumlah yang banyak dan memutuskan jaringan menggunakan tools Mdk3, *Airplay-ng*, loic, dapat dilakukan hasilnya berasil.

2. *Session Hijacking* dengan menggunakan tools Airodump-ng, wireshrak, *cookies* manager. Adapun peneliti melakukan *monitoring* terhadap *client* untuk mendapatkan mac address, dan *cookies* dari target untuk mengambil alih akun yang sedang terkoneksi dengan jairngan *HOTSPOTUBD* dengan menggunakan capture paket pcap. Tools yang peneliti

gunakan Airodump-ng Tidak berasil melakukan session hijacking, wireshark, *cookies* manager berasil mendapatkan cookies dari user lain

3. *Disconnected Computer Client* dengan menggunakan tools netcut dan tuxcut, cara kerjan *Disconnected Computer Client* adalah Memutuskan jaringan *client* dengan menggunakan tools yang ada di windows dan linux, berasil dilakukan dengan logi ke sistem.

4. *Sniffing* dengan menggunakan tools hamster tidak bersil, dengan menggunakan wireshark dan netwitness dapat di lakukan.

3.4.2. Rekomendasi Perbaikan

Berdasarkan beberapa pengujian dengan *scanning* dan *attack* terhadap *HOTSPOTUBD* didapat perbaikan yang harus dilakukan untuk dijadikan rujukan untuk dilakukan perbaikan agar sistem dapat berjalan lebih baik lagi.

1. Recomendasi perbaikan untuk *vulnerable applications version* dari Apache/2.2.12 *appears to be outdated (current is at least* Apache/2.2.22). Apache 1.3.42 *(final release)* and 2.0.64 *are also current* adalah lakukan update untuk menutup vulnerable dari aplikasi.

2. Rekomendasi perbaikan untuk aplikasi *Apache httpd remote denial of service* dari hasil *scanning* dengan menggunakan acunetix belum ada *patch* untuk versi terbaru. Adapun ada pilihan alternatif lain yang dapat dilakukan seperti;

Kode 3.1. rekomendasi perbaikan aplikasi apache remote denial of service

```
a. Use SetEnvIf or mod_rewrite to detect a large number of ranges and then either ignore the Range: header or reject the request.
   Option 1: (Apache 2.0 and 2.2)
      # Drop the Range header when more than 5 ranges.
      # CVE-2011-3192
        SetEnvIf Range (,.*?){5,} bad-range=1
        RequestHeader unset Range env=bad-range
      # optional logging.
   CustomLog logs/range-CVE-2011-3192.log common env=bad-range
   Option 2: (Also for Apache 1.3)
     # Reject request when more than 5 ranges in the Range: header.
      # CVE-2011-3192
      #
   RewriteEngine on
   RewriteCond %{HTTP:range} !(^bytes=[^,]+(,[^,]+){0,4}$|^$)
   RewriteRule .* - [F]
   The number 5 is arbitrary. Several 10's should not be an issue and may be
   required for sites which for example serve PDFs to very high end eReaders or use things such complex http based video streaming.
b. Limit the size of the request field to a few hundred bytes. Note that while
   this keeps the offending Range header short - it may break other headers; such as sizeable cookies or security fields.
     LimitRequestFieldSize 200
     Note that as the attack evolves in the field you are likely to have to further limit this and/or impose other LimitRequestFields limits.
c. Use mod_headers to completely dis-allow the use of Range headers:
   RequestHeader unset Range
   Note that this may break certain clients - such as those used for e-Readers and progressive/http-streaming video.
```

d. *Deploy a Range header count module as a temporary stopgap measure: http://people.apache.org/~dirkx/mod_rangecnt.c Precompiled binaries for some platforms are available at: http://people.apache.org/~dirkx/BINARIES.txt*

---

3. *Application error message*, lakukan *review* terhadap *source code* .
4. Untuk serangan DoS beberapa hal yang harus diperhatikan agak serangan ini dapat diminimalisir kegiatannya dengan menerapkan beberapa hal seperti:

    1. Melakukan *Monitoring* secara berkala terhadap paket – paket yang dikirim oleh *client* .
    2. Melakukan penutupan pada bug-bug dengan cara melakukan patch dan back-up secara berkala. Dengan cara meng*update* patch.
    3. Lakukan blocking terhadap IP yang mencurigakan, jika port target telah termasuki maka komputer target akan di kuasai. Cara mengatasinnya adalah gunakan Firewall di kombinasikan dengan *IDS*.
    4. Menolak semua paket data dan mematikan service *UDP*.
    5. Lakukan *filtering* pada permintaan *ICMP* echo pada *firewall*.

5. Untuk penggunaan *Disconnected Computer Client* bisa dilakukan installasi aplikasi – aplikasi yang mempunyai sistem kerja hampir sama dengan Tuxcut adapun aplikasi – aplikasi diantranya *arpon* bagi pengguna operating system linux. Cara Mengatasi Serangan *Netcut* pada windows adapun beberapa hal yang dilakukan;

    1. Ubah alamat *ip Addres* karena netcut melisting *ip address* di dalam jaringan, maka kamu harus mengganti alamat *ip*. Matikan layanan *workstationb Run*, kemudian ketik services.mscb cari layanan *workstation*. jika sudah ketemu, *klik* kanan, *properties*, *klik* tombol stop.
    2. Ganti *hostname* atau nama komputer anda. *hostname* yang tervisible sangat rentan sekali untuk diserang, oleh karena itu disarankan untuk mengganti dengan hostname yang dekat dengan kepentingan jaringan.
    3. bisa menggunakan *software* bantu/Penangkal. cari *software* anti NetCut atau Anti Arp, sebelum berselancar untuk pertama kali menghidupkan wifi pastikan Anti NetCut atau AntiARP anda telah aktif.
    4. Gunakan *Software* ANTI-NETCUT
    5. Untuk Serangan *Sniffing* gunakan Protokol protokol yang aman seperti IPSec, SMB Signing, HTTPS dan Protokol yang menawarkan keamanan masing – masing.

4. Simpulan

Berdasarkan hasil penelitian yang telah dilakukan pada bab – bab sebelumnya, dalam penelitian ini yang berjudul evaluasi autentikasi pengguna *Wireless LAN* berbasis *Radius Server* Universitas Bina Darma maka penulis menyimpulkan;

1. Pengujian kerentanan pada *HOTSPOTUBD* diperlukan untuk menguji keamanan Wireless LAN Radius Server. Agar memberikan kenyamanan dan keamanan dalam penggunaan fasilitas.
2. Radius Server *HOTSPOTUBD* memiliki tingkat keaman yang tinggi ini dilihat dari beberpa pengujian yang mengarah ke server tidak dapat diakses.
3. Teknik - teknik yang peneliti gunakan masih banyak yang belum dilakukan terhadap *HOTSPOTUBD*.
4. Hasil dari penelitian ini memberikan kontribusi masukan saran perbaikan celah keamanan pada *radius server HOTSPOTUBD*

DAFTAR RUJUKAN

Cartealy, Imam. (2013). *Linux Networking*. Jakarta: Jasakom.

Gunawan. (2006). *Penelitian tindakan kelas proposal, analisis data, monitoring.* Makalah disampaikan pada wokshop

Hassel, Jonathan. (2002). *RADIUS.* Cambridge, Massachusetts : O'Reilly Media.

Sutjipta, Nyoman. 2009. *Agro ergonomi: dasar-dasar ergonomi di bidang pertanian.* Udayana University Press.

Whitaker, A., Newman, D.P., Penetration Testing and Network Defense, diakses pada 1 Desember 2012. Dari http://www.ciscopress.com/store/penetration-testing-and-network-defense-9781587052088