PENETRASI JARINGAN WIRELESS RADIUS HOTSPOTUBD UNIVERSITAS BINA DARMA

Taqrim Ibadi[1], Yesi Novaria Kunang[2], Suryayusra[3]
Dosen Universitas Bina Darma[2,3], Mahasiswa Universitas Bina Darma[1]
Jalan Jenderal Ahmad Yani No.12 Palembang
Pos-el: taqrimibadi91@yahoo.com[1], yesinovariakunang@gmail.com[2],
suryayusra@mail.binadarma.ac.id[3]

ABSTRACT: *Network security is in priority at the moment, considering crime in cyberspace is increasingly vibrant and growing. Her purpose in this study is that wireless security radius can be a little HotspotUBD secured by looking for vulnerabilities by applying the methods of research Action Research which initially stage to identify problems such as theft of data packets and others, and then plan things for penetration will do them (Target Scoping, Information Gathering, Target descovery, enumerating Target, Vulnerability Mapping, Social Engineering, Target Exploitation, Privilege Escalation, Maintaining Access, documentaion and Reporting), then apply the plans that have been made previously. And testing by several techniques, and then evaluate the results of the implementation phase, and a recent study in the principles of the learning criterion. The results of penetration will be considered a network administrator to improve network security loopholes.*

Keywords: *Network Security, Wireless Radius, Penetration.*

ABSTRAK : *Network security* sangatlah di utamakan pada saat ini, menimbang kejahatan di dunia maya semakin hari semakin semarak dan meningkat. Tujuan di buatnya penelitian ini yaitu agar keamanan *wireless radius HotspotUBD* bisa sedikit terjamin keamanannya dengan mencari celah-celah keamanan dengan menerapkan metode penelitian *Action Research* yang mana tahap awalnya melakukan identifikasi masalah seperti pencurian paket data dan lain sebagainya, kemudian merencanakan hal-hal untuk penetrasi yang akan dilakukan (*Target Scoping, Information Gathering, Target Descovery, Enumerating Target, Vulnerability Mapping, Social Engineering, Target Exploitation, Privilege Escalation, Maintaining Access, Documentaion and Reporting*), selanjutnya menerapkan perencanaan yang telah dibuat sebelumnya. Dan melakukan pengujian dengan beberapa teknik, lalu tahap mengevaluasi hasil dari penerapan dan yang terakhir yaitu mempelajari kriteria dalam prinsip pembelajaran. Hasil dari penetrasi akan dijadikan bahan pertimbangan seorang administrator jaringan untuk memperbaiki celah kemanan jaringan tersebut.

Kata Kunci : Keamanan Jaringan, *Wireless Radius*, Penetrasi.

1. PENDAHULUAN

Teknologi *wireless* (tanpa kabel) saat ini berkembang sangat pesat terutama dengan hadirnya perangkat teknologi informasi dan komunikasi. *Komputer, notebook, PDA,* dan telepon seluler (*handphone*) mendominasi pemakaian teknologi *wireless.* Penggunaan teknologi *wireless* yang diimplementasikan dalam suatu jaringan lokal sering dinamakan WLAN (*Wireless Local Area Network*). Namun perkembangan teknologi *wireless* yang terus berkembang sehingga terdapat istilah yang mendampingi WLAN seperti WMAN (*Metropolitan*), WWAN (*Wide*), dan WPAN (*Personal/Private*), Supriyanto (2006:38).

Kementrian Komunikasi dan Informatika Republik Indonesia (2011:48) mengatakan bahwa *Penetration Testing* merupakan suatu proses pengujian yang didesain untuk membobol suatu jaringan menggunakan *tool* dan metodologi-metodologi dari seorang penyerang. *Scanning* kerawanan harus

dilakukan secara berkala, paling tidak mingguan hingga bulanan, dan *penetration testing* harus dilakukan paling tidak tahunan. Sedangkan Hotspot-UBD dari pertamakali diterapkan sampai saat ini belum pernah diuji coba dan oleh karena itulah penelitian ini dilakukan.

Universitas Bina Darma saat ini menggunakan jaringan *Wireless* LAN (Hotspot) RADIUS (*Remote Authentication Dial-In User*) sebagai *wireless security*-nya. Hotspot-UBD menerapkan sistem keamanan menggunakan RADIUS sejak 30 Juli 2010 dan sampai saat ini belum pernah di ujicoba apakah itu sudah aman atau belum dari adanya attacker. Pengujian kemanan secara periodik terhadap sistem sangat penting. Tanpa pengujian secara periodik, tidak ada jaminan terhadap tindakan protektif yang dilakukan atau *patch* pengamanan yang diterapkan oleh administrator berfungsi sebagaimana yang mestinya. Hotspot-UBD merupakan jaringan yang bebas (*public*) yang tersaji untuk siapa saja. Tapi Hotspot-UBD disini khusus untuk dosen dan mahasiswa, itulah mengapa Hotspot-UBD menerapkan sistem keamanan menggunakan RADIUS sebagai *remote dial-up* untuk penggunaan akses jaringan. Dimana RADIUS ini masih menggunakan metode *shared secret* dan sangat beresiko apabila diterapkan untuk proses *autentikasi* dari *client* ke RADIUS server.

Berdasarkan latar belakang diatas, maka penulis merumuskan permasalahan dalam penelitian ini yaitu bagimana menguji keamanan Hotspot UBD sehingga menghasilkan akses data yang aman dari berbagai macam kejahatan.

Agar penelitian lebih terarah dan tidak menyimpang dari permasalahaan yang ada maka perlu adanya batasan masalah. Batasan masalah dalam penelitian ini yaitu yang dipenetrasi adalah jaringan wireless dengan ESSID HotspotUBD khususunya channel 8 lantai 4 yang sedang berjalan di Universitas Bina Darma dan hanya sebatas pengujian (penetrasi) saja dan tidak ada prototype.

Penelitian ini bertujuan untuk mencari celah keamanan yang belum diketahui administrator jaringan sehingga kedepannya bisa meningkatkan keamanan yang ada untuk menghindari hal-hal seperti penyadapan data, akses ilegal oleh orang lain dan memanajemen jaringan Hotspot UBD.

Adapun manfaat dari penelitian ini diantaranya:

1. Bagi pihak Universitas Bina Darma, Penetrasi dilakukan untuk memperbaiki kelemahan yang terdapat pada objek penelitian (Hotspot UBD) sehingga mendapatkan akses data yang lebih aman dari sebelumnya,
2. Bagi Administrator Jaringan, Pentrasi sangatlah penting untuk pengembangan sistem keamanan. Dengan adanya penetrasi, celah-celah terbuka yang belum di ketahui administrator bisa segera di tanggulangi, dan

Bagi Mahasiswa, Penetrasi sangatlah penting, sehingga mahasiswa atau pengguna lebih merasa aman dalam menggunakan layanan *internet* tanpa harus merasa takut akan adanya *attacker* melalui jaringan *wireless*.

2. METODOLOGI PENELITIAN

2.1. Metode Penelitian Tindakan (*Action Research*)

Action Research menurut Davison, Martinsons, dan Kock (2004) yaitu penelitian tindakan yang mendeskripsikan, menginterpretasikan dan menjelaskan suatu situasi sosial atau pada waktu bersamaan dengan melakukan perubahan atau interversi dengan tujuan perbaikan atau partisipasi. Adapun tahapan penelitian yang merupakan bagian dari *action research* ini, yaitu:

1. *Diagnosing*, melakukan *identifikasi* masalah-masalah yang ada guna menjadi dasar kelompok atau organisasi sehingga terjadi perubahan. Penulis melakukan diagnosa terhadap sistem keamanan jaringan *wireless radius Hotspot-UBD* pada Universitas Bina Darma,
2. *Action Planning*, penelitian memahami pokok masalah yang ada, kemudian dilanjutkan dengan menyusun rencana tindakan yang tepat untuk menyelesaikan masalah yang ada. Pada tahap ini peneliti melakukan rencana tindakan yang akan dilakukan pada jaringan *wireless radius* dengan membuat perancangan dan pengujian sistem keamanan jaringan pada Universitas Bina Darma,
3. *Action Taking*, peneliti mengimpelementasikan rencana dengan tindakan yang telah dibuat dengan menjalankan tahapan-tahapan dalam melakukan pengujian terhadap jaringan *wireless radius Hotspot-UBD* untuk mencari kelemahan yang baru dan meningkatkan sistem keamanan jaringan *wireless*,
4. *Evaluating*, setelah masa implementasi (action taking) dianggap cukup, kemudian peneliti melaksanakan evaluasi hasil dari implementasi tadi, dalam tahap ini yang dilihat adalah bagaimana sistem keamanan jaringan *wireless* radius berjalan dengan baik dan sesuai dengan rencana, dan

Specifying Learning, tahap ini merupakan bagian akhir dari siklus yang telah dilalui dengan melaksanakan review tahapan-tahapan yang telah berakhir dan mempelajari kriteria dalam prinsip pembelajaran sehingga penelitian ini dapat berakhir.

2.2. Metode Pengumpulan Data

Dalam melakukan penelitian untuk mendapatkan data dan informasi, maka metode yang digunakan dalam proses pengumpulan data adalah sebagai berikut:

1. Pengamatan (*Observation*), peneliti mengadakan peninjauan langsung ke Universitas Bina Darma khususnya di bagian unit pelaksanaan teknis (UPT-SIM) yang merupakan jantungnya sistem informasi di Universitas tersebut dengan pemilihan, pengubahan, pencatatan, dan pengkodean serangkaian perilaku dan suasana yang berkenaan dengan objek penelitian.
2. Wawancara (*Interview*), untuk mendapatkan informasi dan mendapatkan data-data secara langsung dari sumber yang mengerti sehubungan dengan pengamatan yang penulis lakukan, maka dalam hal ini penulis mengajukan

beberapa pertanyaan-pertanyaan kepada kepala unit pelaksanaan teknis dan beberapa karyawan yang berada disatuan kerja IT Universitas Bina Darma guna mendapatkan informasi berupa gambaran jaringan yang ada disana dan sistem keamanan jaringan *wireless* yang diterapkan di Universitas tersebut sehingga mempermudah penulis dalam mengevaluasi kinerja sistem yang telah dijalankan disana apakah sudah baik atau masih perlu ditingkatkan lagi, dan

Studi Kepustakaan (*Literature*), data diperoleh melalui studi ke pustaka (literature) yaitu dengan cara mencari bahan dari internet, jurnal dan perpustakaan serta buku yang sesuai dengan objek yang akan diteliti.

2.3. Metode Analisis Data Deskriptif

Menurut Nasir (2003:54) bahwa metode deskriptif adalah suatu metode dalam meneliti status sekelompok manusia, suatu objek, suatu set kondisi, suatu sistem pemikiran, ataupun suatu kelas peristiwa pada masa sekarang. Tujuan dari penelitian deskriptif ini adalah untuk membuat deskripsi, gambaran atau lukisan secara sistematis, faktual dan akurat mengenai fakta-fakta, sifat-sifat serta hubungan antarafenomena yang diselidiki.

2.4. Metode Pengujian White Box

White Box testing adalah pengujian yang meperhitungkan mekanisme internal dari sebuah sistem atau komponen (IEEE, 1990). *White Box testing* juga dikenal sebagai pengujian yang struktural, pengujian kotak yang jelas (*clear box testing*), dan pengujian kotak kaca (*glass box testing*) (Beizer, 1995). Konotasi dari *clear box testing* dan *glass box testing* tepatnya menunjukkan bahwa anda memiliki visibilitas penuh terhadap internal kerja dari produk prangkat lunak, khususnya logika dan struktur dari kode.

Pendapat lain mengatakan bahwa *white box testing* adalah *penetration testing* yang dilakukan terhadap sistem atau jaringan dengan tipe *white box*, biasanya informasi-informasi mengenai sistem atau jaringan sudah diketahui. Tetapi hal tersebut tidak serta-merta memberikan kemudahan dalam melakukan penetrasi, hal tersebut tergantung dari tester yang melakukan pengujian menilai sejauh mana kelemahan-kelemahan yang terdapat di dalam sistem atau jaringan.

Selain menggunakana metode penelitian pengujian *White Box*, penelitian ini juga menggunakan *BackTrack Testing Methodology* yang terdiri dari sejumlah langkah yang harus diikuti dalam proses di awal, medial, dan tahap akhir pengujian dalam rangka untuk mencapai sebuah penilaian yang sukses. Diantaranya meliputi penjajakan sasaran (*Target Scoping*), mengumpulkan informasi (*Information Gathering*), penemuan target (*Target Discovery*), menghitung sasaran (*Enumerating Target*), pemetaan kerentanan (*Vulnerability Mapping*), rekayasa sosial (Social Engineering), exploitasi target (*Target Exploitation*), eskalasi hak istimewa (*Privilege Escalation*), memelihara akses (*Maintaining Access*), dan dokumentasi dan pelaporan (*Documentation and Reporting*).

3. HASIL

3.1. Melakukan Tindakan (*Action Taking*)

Setelah sebelumnya peneliti melakukan *diagnosing* dan *action planning* yang hanya sebatas mengidentifikasi target secara umum, sekarang peneliti akan menuangkan seluruh tindakan di dalam bab ini berdasarkan *BackTrack Testing Metodology*.

3.1.1. Exploitasi Target (*Target Exploitation*)

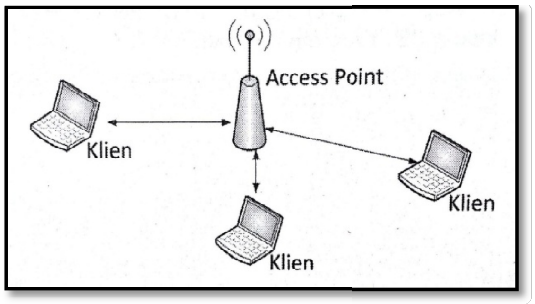
Tabel 3.1 Daftar Hotspot-UBD Kampus Utama Universitas Bina Darma

BSSID	CH	MB	ESSID
C0:C1:C0:0A:0A:CE	1	54	HOTSPOT UBD
68:7F:74:54:75:AE	5	54	HOTSPOT UBD
68:7F:74:A1:4C:53	6	54	HOTSPOT UBD
C0:C1:C0:09:FB:9E	6	54e	HOTSPOT UBD
68:7F:74:54:75:9C	8	54	HOTSPOT UBD
C0:C1:C0:09:F9:A3	10	54	HOTSPOT UBD

Berdasarkan hasil dari peninjauan langsung pada objek penelitian di temukan beberapa *access point* yang terdapat pada kampus utama Universitas Bina Darma yang setiap lantai ditempatkan 1 *access point* untuk HospotUBD seperti yang terlihat pada tabel di atas.

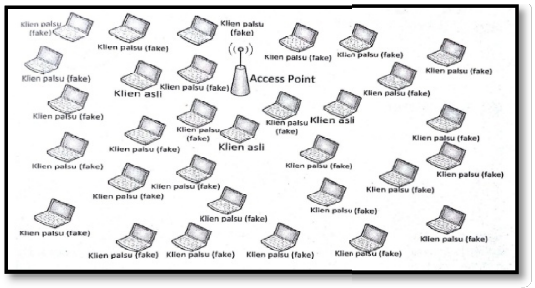
3.1.1.1. *Denial of Service Attack* (DoS) HotspotUBD

Dalam aksi DoS ini, seseorang harus mengirimkan paket *deauthentication* secara terus-menerus, oleh karena itu kenapa aksi ini bisa terjadi. Sewaktu anda mengirimkan banyak paket pada jaringan *wireless* maka *access point* menjadi *overload* sehingga tidak mampu bekerja lagi.



Gambar 3.1 Akses wireless secara normal

Pada gambar 3.1 terlihat bahwa dalam kondisi normal, sebagai contoh katakanlah ada 3 klien yang asli terhubung melalui *access point* pada sebuah jaringan *wireless*.



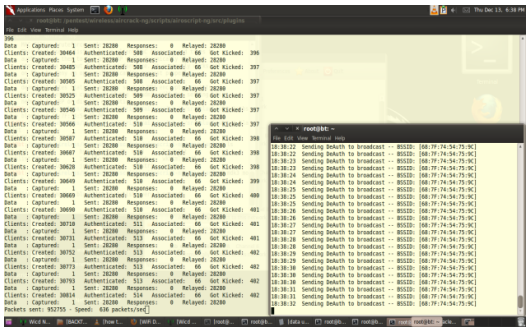
Gambar 3.2 Akses *wireless* secara DoS

Pada tahap ini peneliti melakukan pengujian pada channel 8 BSSID 68:7F:74:54:75:9C dengan pengujian DoS (*Denial of Service Attack*) menggunakan mdk3 tool.

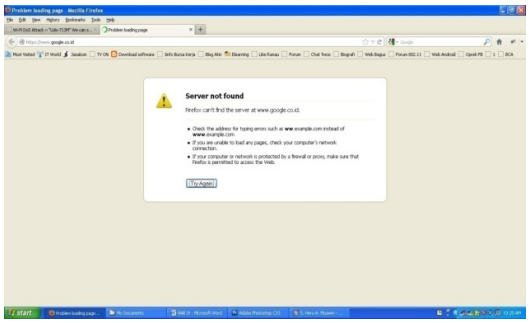
```
#cd /pentest/wireless/aircrack-
ng/scripts/airoscript-
ng/src/plugins/

#mdk3 mon0 d –b blacklist –c
Target_Channel

#mdk3 mon0 a –m –I
Target_Address

#aireplay-ng -0 1000 –a
Target_Address –h My_Address
mon0
```

Sintak di atas berguna untuk menjalankan proses DoS menggunakan tool mdk3. Pada sintak perintah ke-dua bahwa

model jaringan yang kita pakai yaitu *mode monitoring* dan membuat sebuah pengelompokan *blacklist* taget yang akan di serang, begitu juga dengan sintak baris ke-tiga yang memasukkan IP target supaya penyerangan lebih spesifikasi dan terarah. Dan maksud sintak dari perintah *#aireplay-ng* -0 1000 adalah bahwa seorang *attacker* akan mengirimkan paket sebanyak 1000 paket setiap detiknya, sehingga *access point* akan kewalahan dalam menangani setiap paket yang dikirimkan secara terus menerus dan akan menyebabkan access point over load seketika.



Gambar 3.3 Proses DoS pada HotspotUBD dengan 1000 paket/detik



Gambar 3.4 Tampilan Web Browser setelah di DoS

Dampak dari serangan ini bukan hanya belaku bagi *access point* itu sendiri. Tetapi berlaku juga bagi klien yang menggunakan jaringan tersebut. Seperti yang terlihat pada gambar 3.4 bahwa klien mengalami *disconnected* dengan layanan internet ketika ada seorang *attacker* malakukan *Denial of Service Attack.*

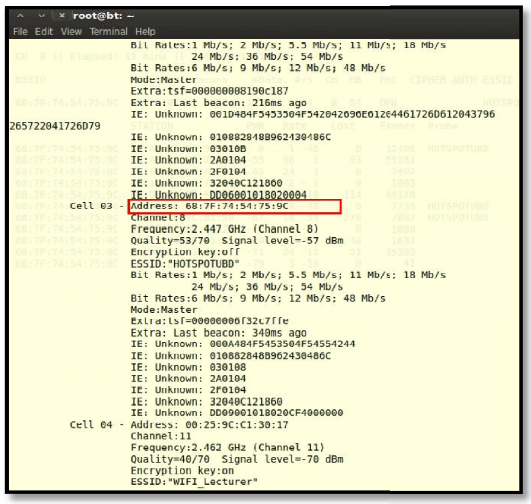
3.1.1.2. *Session Hijacking*

Pengujian kali ini menggunakan teknik *Session Hijacking*, dimana dalam teknik ini *attacker* mengambil kendali session milik user lain setelah sebelumnya mendapatkan MAC Address laptop client dan selanjutnya *attacker* tidak perlu login melalui autentikasi RADIUS. Tools yang digunakan untuk teknik ini yaitu tools yang telah ada pada sistem operasi BackTrack.

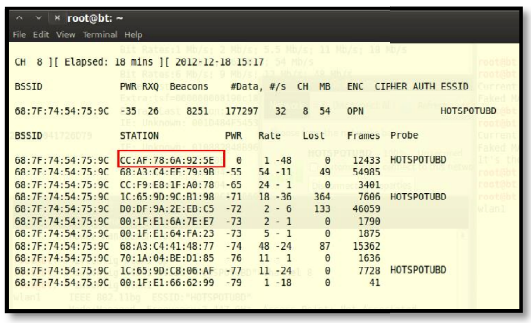
Langkah awal dalam penelitian ini yaitu mencari wireless HotspotUBD dan memonitoring kegiatan dari *wireless* tersebut dengan menjalankan perintah *#iwlist scan.* Dengan perintah diatas, kita bisa melihat informasi MAC target, *chanel* target, ESSID target dan lain sebagainya.

```
#iwconfig wlan1 essid "HOTSPOTUBD" channel 8
#airodump-ng –c 8 –a –bssid 68:7F:74:54:75:9C mon0
```

Pada sintak diatas, maksud dari sintak baris kedua yaitu *attacker* akan melakukan pencarian paket klien atau mencari siapa saja yang terkoneksi ke *access point* HOTSPOTUBD *channel* 8 mengkhususkan MAC *address access point* 68:7F:74:54:75:9C dengan *mode monitoring*.



Gambar 3.5 Menampilkan seluruh Access Point yang terdeteksi

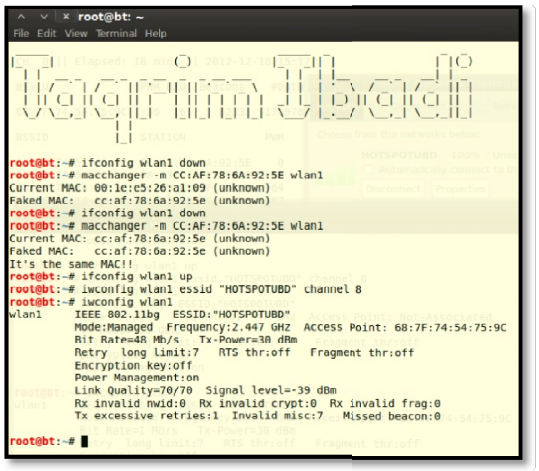


Gambar 3.6 Proses Monitoring WLAN

Sebelum melakukan pemilihan MAC klien untuk target penggantian, satu hal yang perlu di perhatikan yaitu besarnya *packets/frames*. Semakin besar maka semakin besar juga kemungkinan untuk berhasil.

```
#ifconfig wlan1 down
#macchanger –m
CC:AF:78:6A:92:5E wlan1
#ifconfig wlan1 up
#iwconfig wlan1 essid
“HOTSPOTUBD” channel 8
#iwconfig wlan1
```

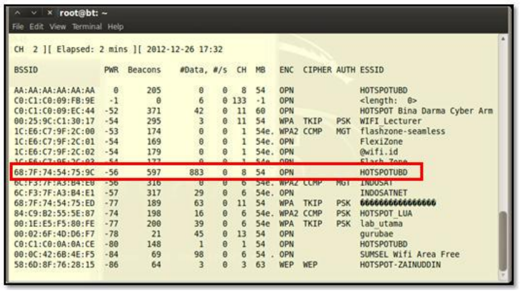
Pada sintak diatas baris ke 2, dimana sintak tersebut berfungsi sebagai pengganti MAC target ke komputer *attacker*. Dan disana attacker memilih MAC target dari klien yang akan digunakan yaitu CC:AF:78:6A:92:5E.



Gambar 3.7 Proses pengubahan MAC Address

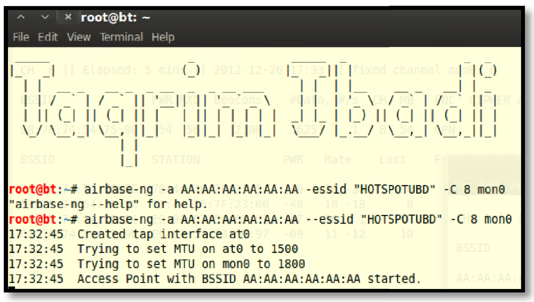
3.1.1.3. *Evil Twin* dan *Access Point MAC Spoofing*

Salah satu serangan yang paling ampuh pada infrastruktur WLAN adalah Evil Twin. Idenya adalah pada dasarnya untuk memperkenalkan titik penyerang yang dikendalikan akses di sekitar jaringan WLAN. Jalur akses ini akan mem-*broadcast* SSID yang sama persis seperti resmi jaringan WLAN. Banyak pengguna nirkabel terhubung ke akses jalur berbahaya ini dan berfikir ini adalah bagian dari jaringan yang sah atau resmi. Setelah sambungan dibuat, penyerang dapat mengatur sebuah aktifitas *man-in-the-middle attack* dan sementara menguping seluruh komunikasi lalu lintas transparan estafet.



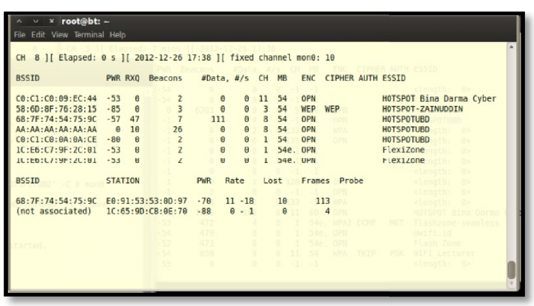
Gambar 3.8 Proses pencarian BSSID Target

Dengan menggunakan informasi ini, kita akan membuat jalur akses baru dengan ESSID yang sama tetapi BSSID yang berbeda dan alamat MAC menggunakan perintah *airbase-ng*.



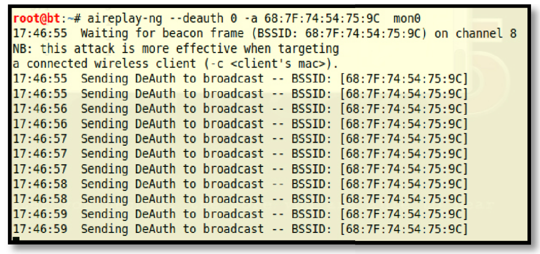
Gambar 3.9 Membuat jalur akses baru

Jalur akses baru ini juga muncul di layar *airodump-ng*. Hal ini penting untuk dicatat bahwa anda akan perlu menjalankan airodump-ng di jendela baru untuk melihat jalur akses baru.

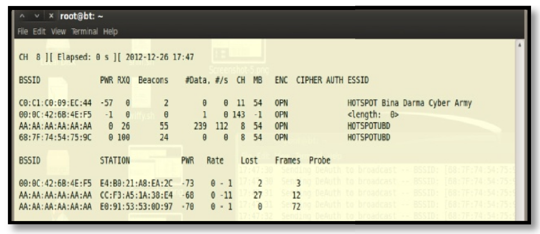


Gambar 3.10 Melihat jalur akses baru

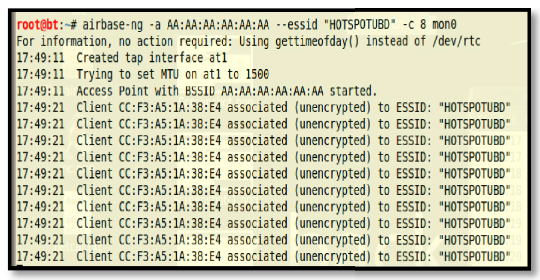
Tahap selanjutnya yaitu mengirim *frame De-Otentikasi* ke *access point* asli yang terkoneksi 68:7F:74:54:75:9C, sehingga memutuskan dan segera mencoba untuk menghubungkan kembali.



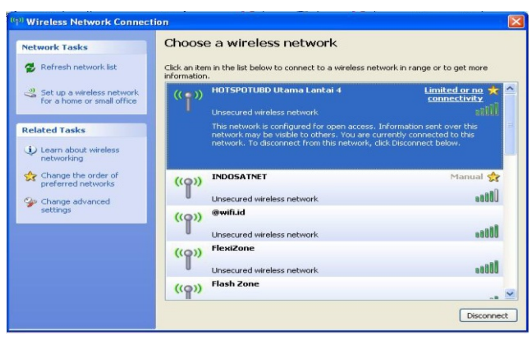
Gambar 3.11 Proses mengirim *De-Otentikasi* ke klien



Gambar 3.12 Data lebih banyak di bandingkan yang asli



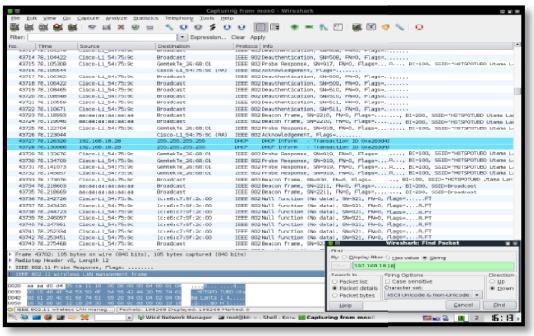
Gambar 3.13 Kekuatan sinyal lebih tinggi dari yang asli



Gambar 3.14 Koneksi klien terputus sementara

Koneksi pada klien terputus sementara, setelah teknik evil twin di eksekusi. Klien harus koneksi kembali dengan AP dan

disinilah hasil attacker menunjukkan hasil. Karena pada saat klien melakukan koneksi terhadap AP, sinyal jaringan sedang tidak stabil karena ada 2 AP yang sama dimulai dari MAC, ESSID, dan lain sebagainya.



Gambar 3.15 Attacker menangkap paket klien

Karena klien sebelumnya sudah terkoneksi dengan AP, selanjutnya klien tidak perlu login dengan AP yang sama dengan menggunakan fasilitas cookies pada browser. Dan disinilah keuntungan attacker untuk mengecoh target. Selanjutnya attacker akan menangkap paket klien dengan menggunakan mode monitoring pada laptop attacker, sehingga seluruh aktifitas klien pada jaringan akan terdeteksi oleh attacker dan selanjutnya menggabungkan teknik-teknik yang lain untuk melakukan penyerangan yang lebih pada target.

3.1.1.4. SQL Injection

SQL (Structure Query Language) digunakan untuk pengelolaan database dengan cara mengirimkan perintah (query) yang terstruktur. SQL Injection merupakan sebuah aksi hacking yang dilakukan di aplikasi client dengan cara memodifikasi perintah atau sintak SQL.

Tabel 3.2 Variasi kode lain dari *SQL Injection*

Admin'--	or 0=0 #	or 1=1 --	hi" or 1=1 --
' or 0=0 --	' or 'x'='x	' or a=a --	hi' or 1=1 --
" or 0=0 --	" or "x"="x	" or "a"="a	hi' or 'a'='a
or 0=0 --	') or ('x'='x	') or ('a'='a	hi') or ('a'='a
' or 0=0 #	' or 1=1 --	") or ("a"="a	hi") or ("a"="a
" or 0=0 #	" or 1=1 --	hi" or "a"="a	

Disini peneliti mencoba menggunakan teknik ini pada portal web autentikasi *wireless* RADIUS HOTSPOTUBD dengan memasukkan sintak SQL pada *hotspotlogin.php*.

Gambar 3.16 Proses memasukkan sintak *SQL Injection*

Setelah sintak di eksekusi pada portal tersebut, sebagian ada yang masih tetap seperti biasa tidak ada yang di tampilkan, dan ada beberapa sintax yang jika di eksekusi akan otomatis ke IP Gateway *access point* dengan port 3990.

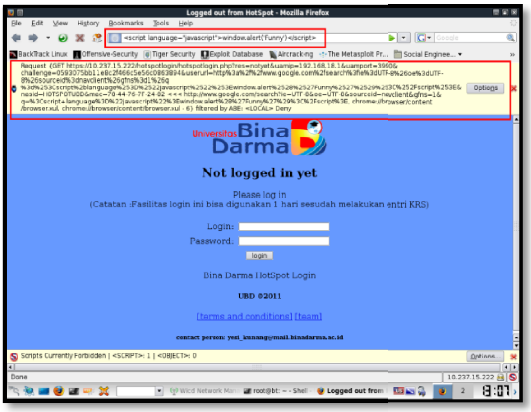
Gambar 3.17 Hasil eksekusi sintak *SQL Injection*

3.1.1.5. XSS (*Cross-Site Scripting*)

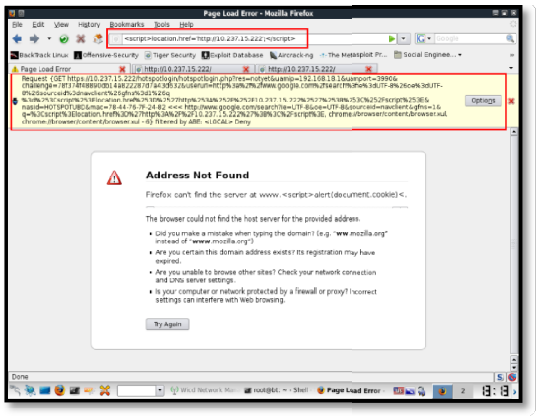
Teknik ini dilakukan dengan cara menginjeksi atau memasukkan script ke dalam website melalui sebuah browser. Aksi XSS ini adalah dengan memanfaatkan metode HTTP GET/HTTP POST. Pada penelitian ini, script dicobakan pada portal auntentikasi untuk mengetahui apakah portal tersebut bisa di XSS atau tidak, dengan memasukkan script:

```
<script
language=”javascript”>window.al
ert(‘Percobaan, berhasil atau
tidak’)</script>

<script>location.href=’http://1
0.237.15.222’;</script>
```

Sintak pertama berfungsi untuk memeriksa apakah portal bisa diserang dengan teknik ini, jika sintak di eksekusi dan jika portal bisa diserang maka akan ada tampilan baru yang memuat tulisan ‘Percobaan berhasil atau tidak’ sesuai dengan perintah yang kita masukkan sebelumnya. Kemudian untuk sintak yang ke-dua berguna mencari *cookies* untuk IP 10.237.15.222.



Gambar 3.18 Hasil eksekusi script 1

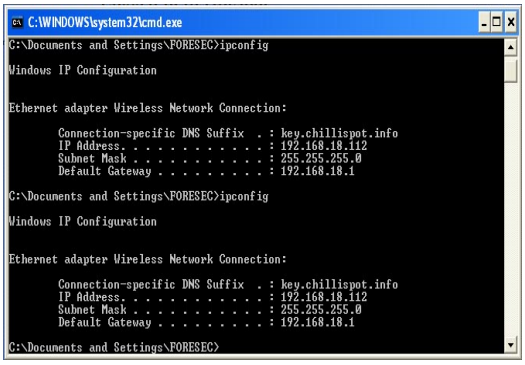


Gambar 3.19 Hasil eksekusi script 2

Dari tindakan di atas, kita mengetahui bahwa target tidak bisa di XSS, berarti tidak bisa pula di-*redirect* ke halaman lain.

3.1.1.6. *Disconnected Computer Client*

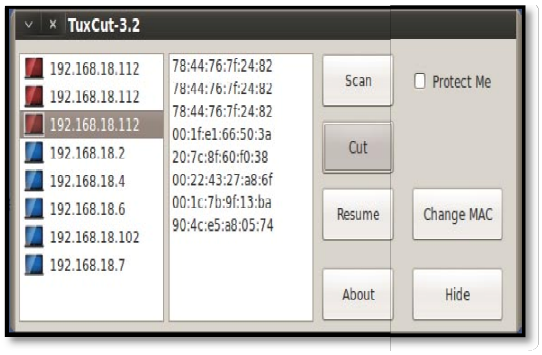
Penelitian yang satu ini yaitu melakukan pemutusan jaringan client dimana peneliti menggunakan *tools* TuxCut pada Operating System BackTrack5 untuk melakukan teknik ini. Sekilas cara kerja TuxCut ini adalah menjadikan laptop atau komputernya sebagai gateway. Sehingga dia bebas mengatur siapa yang masuk, dan siapa yang perlu dikeluarkan (*disconnect*). Dan untuk melakukan teknik ini *attacker* memerlukan koneksi terlebih dahulu ke *access point* dan mendapatkan IP dari AP.



Gambar 3.20 Melihat IP Target

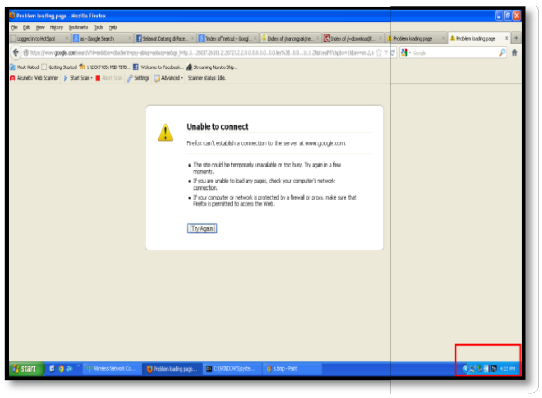
Gambar 3.20 menunjukkan IP dari target yang nantinya akan kita putuskan koneksinya dengan internet secara paksa. Dan

disana terlihat IP dari target adalah 192.168.18.112.



Gambar 3.21 Proses pemutusan jaringan klien

Pada gambar 3.21 untuk IP *attacker* yaitu 192.168.18.7 dengan MAC *address* 90:4C:E5:A8:05:74 akan melakukan pemutusan koneksi klien dengan IP 192.168.18.112 MAC *address* 78:44:76:7F:24:82.



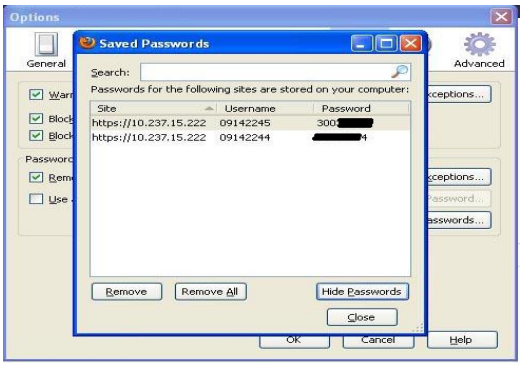
Gambar 3.22 Hasil setelah eksekusi

Gambar 3.22 menunjukan tampilan klien yang setelah dilakukan pemutusan jaringan menggunakan TuxCut dan terlihat pada *icon wireless network connection* pada sudut kanan bawah terjadi proses pencarian ulang koneksi terhadap *access point*.

Gambar 3.22 Proses pencarian ulang koneksi internet

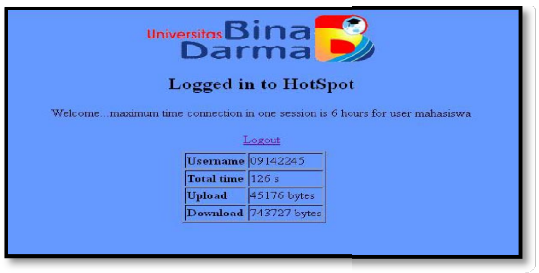
3.1.1.7. *Computer Based Social Engineering*

Pada teknik ini lebih mengonsentrasikan diri pada rantai terlemah sistem jaringan komputer, yaitu manusia. Seperti yang kita ketahui, tidak ada sistem komputer yang tidak melibatkan interaksi manusia. Teknik ini bergantung pada *software* yang digunakan untuk mengumpulkan data atau informasi yang diperlukan. Pada penelitian ini, peneliti mengumpulkan data dari komputer salah satu klien yang sudah pernah terkoneksi pada jaringan HOTSPOTUBD.



Gambar 3.23 Password yang tersimpan pada software Mozillla Firefox

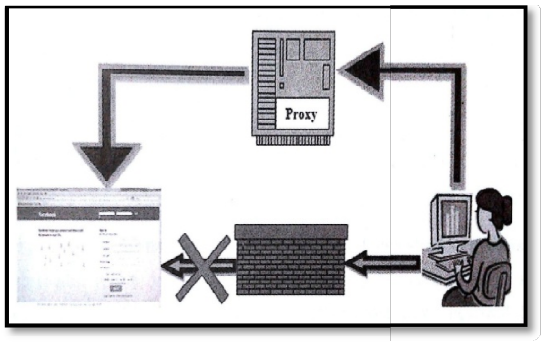
Gambar 3.23 menunjukkan bahwa untuk alamat https://10.237.15.222 akses loginnya tertera disana secara jelas. Ini bisa terjadi jika sipengguna malas untuk mengingat data-data yang begitu penting dan rentan terhadap kejahatan tersebut.



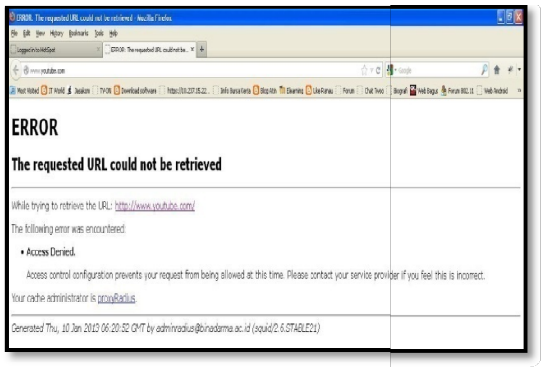
Gambar 3.24 Hasil pengujian untuk *Username* dan *Password*

3.1.1.8. *Anonymouse Browsing*

Teknik ini menggunakan web yang khusus bersifat anonymous. Dimana dalam penelitian ini yang digunakan adalah web proxy. Kita tidak perlu menggonta-ganti settingan proxy tinggal menggunakan jasa web proxy untuk menggunakan internet secara *bypass*. Bypass disini maksudany kita bisa membuka situs-situs yang pada awalnya tidak bisa dibuka seperti membuka alamat *youtube.com*, dan *facebook.com*.

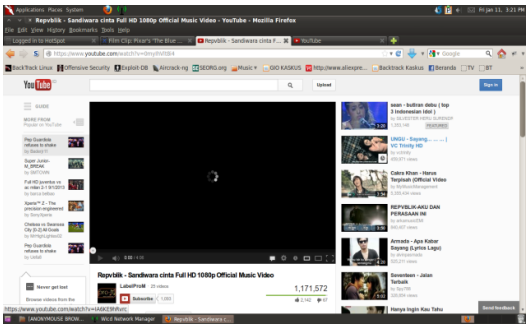


Gambar 3.25 Membuka situs yang di blokir



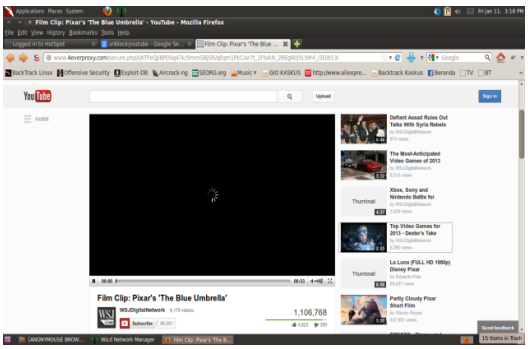
Gambar 3.26 Salah satu situs yang di blokir

Gambar 3.26 menunjukkan pemblokiran pada salah satu situs yaitu *youtube.com* demi kenyamanan dalam menggunakan internet selama proses belajar mengajar berlangsung.



Gambar 3.27 *Bypass* situs *youtube.com*

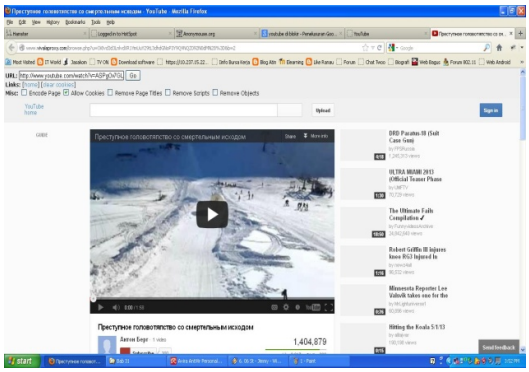
Dengan menambahkan karakter “s” pada http menjadi https, sehingga alamat *youtube.com* bisa dibuka seperti biasa. Dan hal ini berlaku juga untuk alamat situs yang di blokir lainnya seperti *facebook.com*, *google.com*, *twitter.com*. Ini bisa secara otomatis di gunakan tanpa harus mengetik manual karakter “s” pada http, kita tinggal mengupdate web browser kita. Karena demi keamana pengguna, web browser telah mengupdate softwarenya dengan selalu menggunakan https bukan http.



Gambar 3.28 Menggunakan web proxy situs *www.4everproxy.com*

Beberapa situs menyediakan fasilitas untuk membuka alamat-alamat situs yang diblokir pada suatu jaringan. Pada penelitian ini, menggunakan dua situs untuk mencobanya

yaitu: *www.4everproxy.com* dan *www.vivalaproxy.com*.



Gambar 3.29 Menggunakan web proxy situs *www.vivalaproxy.com*

3.1.2. Eskalasi hak Istimewa (*Privilege Escalation*)

1. Menggunakan *Tools* Droidsheep SmartPhone Android

Kegiatan ini bertujuan untuk pengujian keamanan data *client* dan untuk kenyamanan *client* dalam menggunakan fasilitas *wireless* yang disediakan. Pada tahap ini penelitian dilakukan menggunakan tools yang terdapat pada handphone smartphone yang mana tools tersebut akan menampilkan ID *client* yang sedang berselancar di dunia maya khususnya sedang menggunakan jaringan sosial (*facebook.com*), layanan *e-mail* (*yahoo.com*), dan *search engine* (*google.com*). Tools ini akan melakukan *ARP-Spoofing* kepada *access point* dan membutuhkan *login* ke RADIUS telebih dahulu.

Gambar 3.30 Tampilan pada Web Browser sebelum dan sesudah login

Gambar 4.34 akan menunjukkan bahwa memang sudah benar terkoneksi dengan *access point* yang di tuju dengan menampilkan halaman depan pengaksesan dari *access point* tersebut, dan dilanjutkan dengan menampilkan proses ARP-*Spoofing* pada IP 192.168.18.1 dimana IP tersebut merupakan IP *gateway* dari *access point*.

Gambar 3.31 Tampilan port 80 dari *access point* dan proses *ARP-Spoofing*

Gambar 3.31 menampilakan *client* yang ter-*sniffing* dan kedapatan sedang membuka situs jejaringan facebook. Disana peneliti mencoba melakukan update status melalui handphone peneliti dengan memasukkan status "Sniffing" dan hasilnya langsung terlihat disana dengan ter-update nya status akun facebook target.

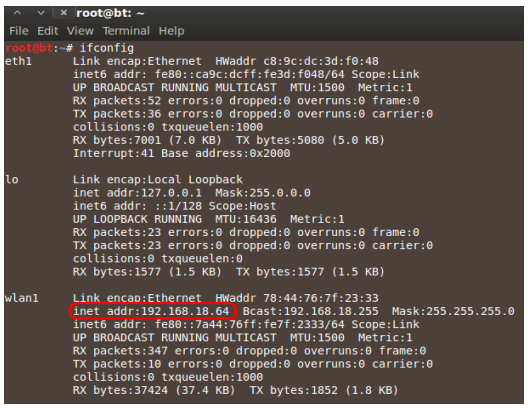
Gambar 3.32 Client yang ter-sniffing

2. Menggunakan Tools Ettercap BackTrack

Ettercap merupakan salah satu tools yang banyak digunakan untuk melakukan kegiatan yang bersifat mengintip kegiatan klien melalui jaringan (*sniffing*). Dan biasanya Ettercap di terapkan pada LAN bukan di WLAN, tapi untuk penelitian ini dilakukan pengujian pada WLAN.

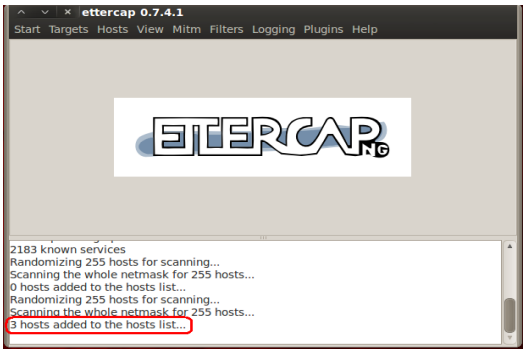
Gambar 3.33 Pengujian tanpa Login Autentikasi

Gambar 3.33 menunjukkan untuk pengujian yang satu ini tanpa Login Autentikasi dan pengujian ini bersifat eksternal.

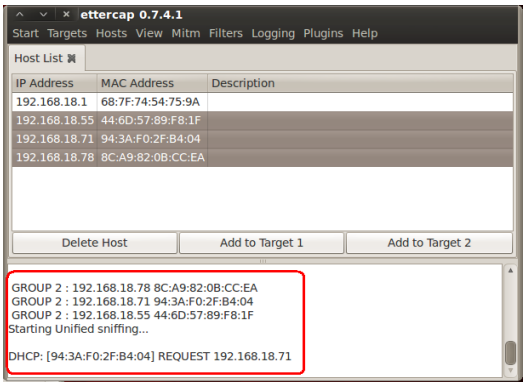


Gambar 3.34 Melihat IP Attacker

IP di atas kita dapatkan setelah melakukan koneksi dengan HotspotUBD walaupun tanpa Login melalui auntentikasi RADIUS.



Gambar 3.35 Proses melihat jumlah Host yang terkoneksi dengan HotspotUBD

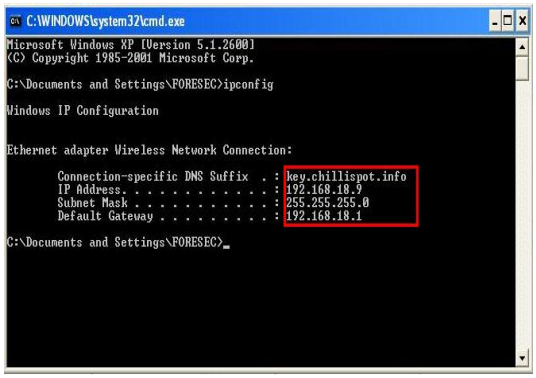


Gambar 3.36 Proses Sniffing tidak berhasil

Gambar 3.36 menunjukkan bahwa proses sniffing paket client menggunakan Ettercap tidak berhasil karena yang terdeteksi hanya DHCP Request dari IP Client.

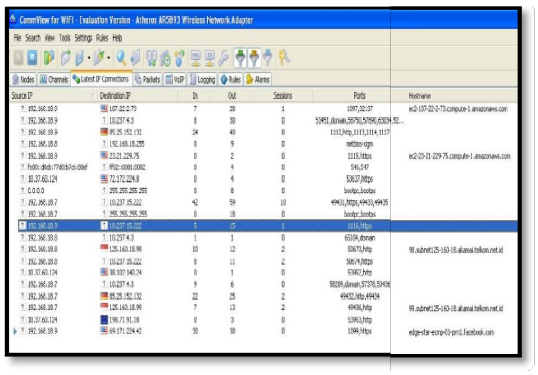
3. Menggunakan *Tools SmartWhois* dan *CommView for WiFi*

Fungsi salah satu dari *software* ini adalah berguna untuk memantau jaringan *wireless* 802.11 a/b/g/n. Baik itu berupa pemantauan dari aktifitas *client* sampai dengan jenis atau tipe *hardware* dari *access point* yang terdeteksi. Untuk menggunakan software ini, seorang *attacker* tidak musti harus *login* dengan autentifikasi RADIUS terlebih dahulu, cukup mendapat IP dari AP dan selanjutnya melakukan penangkapan paket klien.



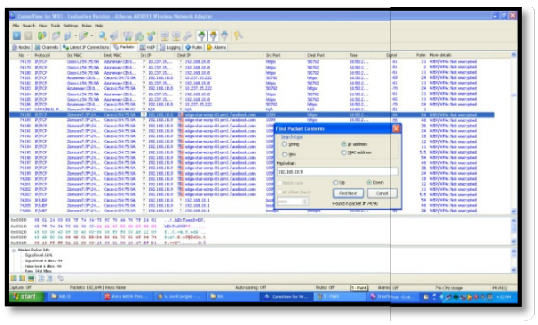
Gambar 3.37 IP Target

Selanjutnya dengan gambar 3.37 kita bisa melihat IP dari target yang akan kita serang dengan IP 192.168.18.9 dengan *default gateway* 192.168.18.1.



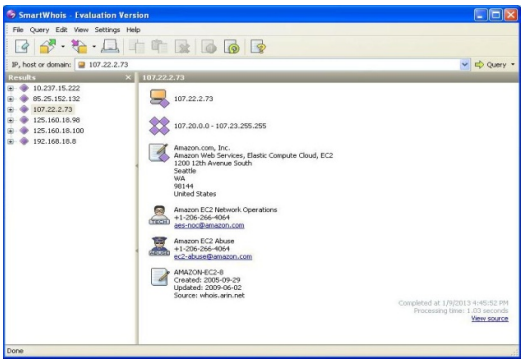
Gambar 3.38 Aktifitas dari IP yang terkoneksi ke AP

Gambar 3.38 menunjukkan bagaimana proses penangkapan paket klien melalui jaringan yang digunakan target. Tools ini hampir sama dengan wireshark dimana fungsinya sama-sama menangkap paket jaringan dan kemudian bisa di analisa lebih lanjut.



Gambar 3.39 Hasil penelusuran paket IP 192.168.18.9

Pada 3.39 menunjukkan hasil tangkapan paket dari seluruh aktifitas client yang sedang menggunakan layanan internet. Dalam hal ini, yang merupakan situs yang di kunjungi biasanya adalah port *http* atau *https*.



Gambar 3.40 Informasi yang ditampilkan menggunakan tools SmartWhois

3.2. Melakukan Evaluasi (*Evaluating*)

3.2.1. *Maintaining Access*

Kalau pada eskalasi hak istimewa (*privilege escalation*), peneliti menguji bagaimana cara untuk mengakses ke mesin target. Tapi pada tahapan ini, peneliti akan menyimpulkan bagaimana mengakses mesin target kapanpun *attacker* mau. Inti pada tahapa ini yaitu, bagaimana attacker membuat sebuah celah untuk mendapatkan hak aksesnya kembali jika suatu saat attacker membutuhkan. Dan kebetulan, pada penelitian ini khususnya tahapan *maintaining access* seperti mengakses user password di RADIUS tidak bisa peneliti tampilkan karena keterbatasan informasi yang didapatkan dari pengujian dan juga keterbatasan sistem yang bisa ditembus oleh peneliti kecuali, dengan teknik *social engineering* yang memanfaatkan kesalah dari manusia itu sendiri.

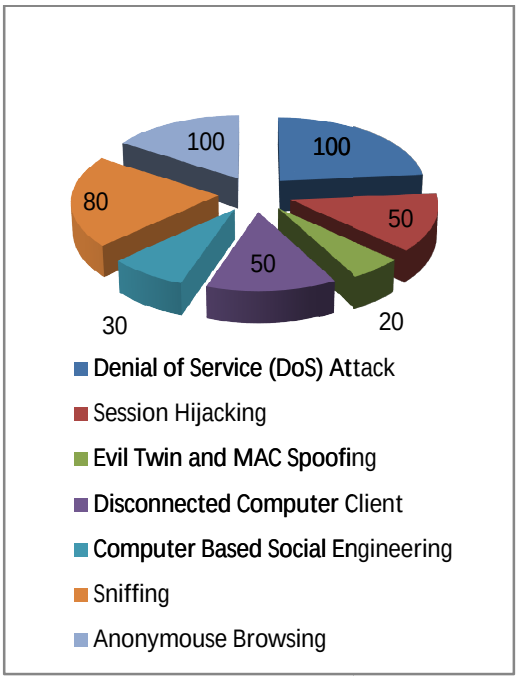
Setelah dilakukan analisis dengan teknik social engineering pada autentifikasi RADIUS bahwa *user* adalah NIM mahasiswa itu sendiri sedangkan password tergantung dari password mahasiswa di sistem akademis.. Jadi untuk kedepannya jika kita ingin menggunakan atau masuk ke database mahasiswa itu sendiri cukup mencari *user* yang masih menggunakan *user* dan *password login default*. Dan ternyata *user* dan *password default* tersebut juga terkoneksi atau berguna untuk membuka situs-situs akademik dari Universitas Bina Darma itu sendiri, baik untuk melihat tugas kuliah maupun melihat nilai dari mahasiswa itu sendiri. Dan ini akan membuat seorang *attacker* semakin leluasa terhadap suatu *account* yang masih menggunakan *user* dan *password default*. Begitu juga untuk login pada autentifikasi RADIUS HotspotUBD Universitas Bina Darma.

Gambar 3.41 Tampilan database mahasiswa dari website *binadarma.ac.id*

Gambar 3.41 menunjukkan tampilan suatu *account user* yang mana peneliti mencoba untuk membuka situs *binadarma.ac.id* dengan menggunakan *user* dan *password* secara acak mencari yang masih *default* dengan memanfaatkan teknik *social engineering*.

3.3. Pembelajaran (*Learning*)

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



Gambar 3.42 Statistik keberhasilan teknik berdasarkan pengujian

Statistik keberhasilan di hitung berdasarkan berapa kali pengujian terhadap objek. Dimana pengujian di lakukan sebanyak 10 kali.

Tabel 3.3 Table Hasil Pengujian

NO	JENIS SERANGAN	TOOLS	HASIL	STATUS
1	Denial of Service Attack (DoS)	mdk3, aireplay -ng	BERHASIL	TIDAK LOGIN
2	Session Hijacking	airodump-ng	BERHASIL	TIDAK LOGIN
3	Evil Twin dan Access Point MAC Spoofing	airbase-ng, airplay-ng, airodump-ng	BERHASIL	TIDAK LOGIN
4	SQL Injection		TIDAK BERHASIL	TIDAK LOGIN
5	XSS (Cross-Site Scripting)		TIDAK BERHASIL	TIDAK LOGIN
6	Disconnecte	TuxCut	BERHASIL	LOGIN

	d Computer Client			
7	Computer Based Social Engineering	Browser Mozilla Firefox	BERHASIL	TIDAK LOGIN
8	Sniffing	Droidsh eep	BERHASIL	LOGIN
		Ettercap	TIDAK BERHASIL	LOGIN
		SmartW hois dan CommV iew for WiFi	BERHASIL	TIDAK LOGIN
9	Anonymous e Browsing		BERHASIL	LOGIN

4. SIMPULAN

Berdasarkan hasil penelitian dan pembahasan yang telah diuraikan pada bab sebelumnya, dalam penelitian yang berjudul Penetrasi Jaringan *Wireless* RADIUS HotspotUBD Universitas Bina Darma, maka dapat disimpulkan:

1. Hasil penelitian ini yaitu memberikan kontribusi saran perbaikan celah keamanan pada sistem RADIUS HotspotUBD.
2. Teknik pengujian dalam jaringan HotspotUBD masih begitu banyak yang belum dicobakan pada penelitian ini dan itu berarti belum semua celah pada jaringan *wireless* RADIUS HotspotUBD yang peneliti temukan.
3. Penggunaan mode RADIUS pada jaringan *wireless* HotspotUBD merupakan jenis kemanan yang sulit untuk ditembus bagi *attacker* pemula, apalagi sampai untuk mengakses atau masuk kedalam sistem server RADIUS.
4. Penelitian dilakukan pada *channel* 8 lantai 4 kampus utama karena, menurut analisa peneliti berdasarkan banyaknya pengguna dan di sesuaikan dengan pembatasan *bandwidth* pada seatiap channel oleh administrator jaringan, lalulintas paket data untuk *channel* 8 yang bertebaran di udara pada saat penelitian dilakukan, peneliti menyimpulkan bahwa waktu itu sangat sesuai untuk menerapkan teknik-teknik yang akan dilakukan di bandingkan pada *channel* yang lainnya.

5. DAFTAR RUJUKAN

Ali, Shakel., Heriyanto, Tedy. (2011). BackTrack 4: *Assuring Security by Penetration Testing*. Birmingham-Mumbai: PACK Publishing Open Source.

Arifin, Zaenal. (2008). Sistem Pengamanan Jaringan *Wireless* LAN Berbasis Protokol 802.1x dan Sertifikat.

Davison, R.M., Martinsons, M.G., Kock N. (2004). Jurnal: *Information Systems* dan *Principles of Canonical Action Research.*

Dipanegara, Arya. (2011). Cara Instan Jago *Hacking*. Jakarta Barat: Agogos Publishing.

ID-SIRTII. (2012). Pemantauan Trafik Nasional. (*http://berita.idsirtii.or.id/category/berita*/, diakses 15 Oktober 2012).

Kementrian Komunikasi dan Informatika Republik Indonesia. (2012). E-Book: Panduan Keamanan Web Server.

Kunang, Yesi Novaria dan Yadi, Ilman Zuhri. (2008). Jurnal: Autentikasi Pengguna Wireless LAN Berbasis RADIUS Server pada WLAN Universitas Bina Darma, Dosen Tetap Universitas Bina Darma.

Nasir, Moh Ph.D. (2003). Metode Penelitian. Jakarta: Ghalia Indonesia.

Penerbit ANDI. (2012). *Network Hacking* dengan *Linux BackTrack*. Semarang: Wahana Komputer.

Ramachandran, Vivek. BackTrack5 *Wireless Penetration Testing*. Birmingham-Mumbai: PACK Publishing Open Source.

Sofana, Iwana. (2010). CISCO CCNA & JARINGAN KOMPUTER. Bandung: Informatika.

Struktur Organisasi UPT-SIM Universitas Bina Darma (*Online*), (*http://binadarma.ac.id/content/120/0/miscuts.html*, diakses 28 September 2012).

Sugiyono. (1999). Metode Penelitian Bisnis. Bandung: ALFABETA.

Supriyanto, Aji. (2006). Jurnal: Analisis Kelemahan Keamanan pada Jaringan Wireless. Universitas Stikubank Semarang.

Thomas, Tom. (2005). *Network Security First-Step*. Yogyakarta: Andi OFFSET

Zam, Efvy. (2012). Buku Sakti Hacker. Jakarta Selatan:Mediakita.

Zam, Efvy. (2012). *Wireless Hacking*. Jakarta: PT Elex Media Komputindo.