PENETRASI JARINGAN WIRELESS RADIUS

SURYAYUSRA, M.Kom UNIVERSITAS BINA DARMA

Latar Belakang Masalah

Teknologi *wireless* (tanpa kabel) saat ini berkembang sangat pesat terutama dengan hadirnya perangkat teknologi informasi dan komunikasi. 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.

Objek penelitian 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.

Dasar Teori

Penetrasi adalah suatu kegiatan untuk melakukan pengecekan *vulnerability* (celah keamanan) dari suatu *network, device, server.* Penetrasi jaringan sangat diperlukan untuk meminimalisasi celah keamanan yang belum diketahui dan merupakan langkah awal yang sangat bagus bagi sebuah organisasi yang sangat mempertimbangkan pentingnya pemahaman keamanan pada jaringan mereka dan efektivitasnya. Dengan begitu, seseorang yang tidak punya hak tidak akan mudah masuk ke sistem jaringan.

Zam (2012:4) secara konsisten menyatakan banyak yang mengira bahwa jaringan *wireless* lebih aman daripada jaringan kabel. Pernyataan tersebut tidak sepenuhnya benar, juga tidak sepenuhnya salah, karena pada dasarnya aktivitas *hacking* pada jaringan *wireless* lebih mudah daripada jaringan kabel, sebab seseorang bisa terkoneksi melalui sebuah jaringan *wireless*, kapanpun dan dimananpun selagi terdapat jaringan *wireless*. Selain itu, keberadaan seseorang yang terhubung melalui jaringan *wireless* juga susah diketahui di mana keberadaannya. Lain halnya dengan jaringan kabel, seseorang tentu saja harus terhubung secara fisik barulah mereka bisa melakukan aksi *hacking*.

Solusi dan Metode Penelitian

Solusi dari masalah yang ada adalah 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.

Metode Penelitian meliputi antaralain:

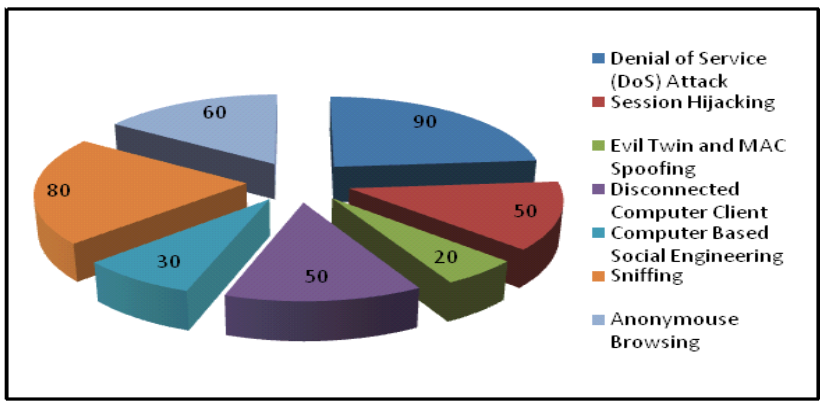
1. Metode Penelitian Tindakan (*Action Research*),

2. Metode Pengumpulan Data yang terdiri dari, Pengamatan (*Observation*), Wawancara (*Interview*), dan Studi Kepustakaan (*Literature*).

3. Metode Analisis Data Deskriptif,

4. Metode Pengujian White Box. 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*).

Hasil



Gambar Statistik keberhasilan teknik berdasarkan pengujian

NO	JENIS SERANGAN	STATUS	KONEKSI
1	Denial of Service Attack (DoS)	Berhasil	Tidak Login
2	Session Hijacking	Berhasil	Tidak Login
3	Evil Twin dan Access Point MAC Spoofing	Berhasil	Tidak Login
4	SQL Injection	Tidak Berhasil	Tidak Login
5	XSS (Cross-Site Scripting)	Tidak Berhasil	Tidak Login
6	Disconnected Computer Client	Berhasil	Login
7	Computer Based Social Engineering	Berhasil	Tidak Login
8	Sniffing	Berhasil	Login dan Tidak Login
9	Anonymouse Browsing	Berhasil	Login

Kesimpulan dan Rekomendasi

A. **Kesimpulan**

Hasil penelitian ini yaitu memberikan kontribusi saran perbaikan celah keamanan pada sistem RADIUS HotspotUBD. 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. 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.

B. **Rekomendasi**

Perlunya edukasi bagi pengguna HotspotUBD terutama untuk celah keamanan *session hijacking*, *evil twin*, *computer based social engineering*, *sniffing*, dan *social engineering*. Misalnya user di edukasi untuk merubah *password* yang lebih aman.

Monitoring administrator jaringan sangat diperlukan guna memantau setiap pergerakan paket yang dilakukan oleh klien.

Pengupdatean *firewall* pada jaringan sangan diperlukan dan juga pengupdatean *blocking site* agar klien jaringan terbebas dari website yang berkonten pornograpi maupun website yang diluar sistem akademik.