HIJACKING SESSION TERHADAP SISTEM INFORMASI AKADEMIK UNIVERSITAS ISLAM NEGERI RADEN FATAH PALEMBANG

Febriyanti Panjatan[1], Aldian Muziwansyah[2], Fatoin[3]

[1,2,3]Jurusan Teknik Informatika, Universitas Bina Darma
Email: febriyanti_panjaitan@binadarma.ac.id

ABSTRAK

Perkembangan Sistem Informasi Akademik (Simak) yang semakin cepat dengan berbagai macam fungsi dan kebutuhan, menuntut meningkatnya kualitas keamanan jaringan simak online. Universitas Islam Negeri (UIN) Raden Fatah Palembang memiliki simak online yang terbagi menjadi sembilan bagian menurut fakultas masing-masing yang berfungsi mengelola seputar sistem informasi mahasiswa seperti file mahasiswa, form nilai (KHS), penjadwalan, pengumuman atau informasi kampus dan sebagainya. Simak online tersebut pernah mengalami serangan hacker pada bulan Mei 2016 dimana hacker menyusup pada bagian sistem akademik dengan mengubah tampilan halaman depan dan melakukan perubahan nilai serta saat diakses sering mengalami koneksi yang lambat serta terkadang koneksi yang terputus. Berdasarkan data hasil pengujian penyusupan (Hijacking Session) login user website Sistem Informasi Akademik (Simak) online Universitas Islam Negeri (UIN) Raden Fatah sangat rentan terhadap serangan ARP Spoofing, hal ini dibuktikan saat pengujian dimana user account dan password dapat dilihat pada saat menggunakan aplikasi Ettercap. Untuk meningkat keamanan Web Sistem Informasi Akademik (Simak) online Universitas Islam Negeri (UIN) Raden Fatah, perlunya menggunakan sistem security atau enkripsi seperti teknologi SSL (Secure Socket Layer).

Kata kunci: Hijacking Session, ARP Spoofing, Secure Socket Layer

1. PENDAHULUAN

Perkembangan Sistem Informasi Akademik (Simak) yang semakin cepat dengan berbagai macam fungsi dan kebutuhan, menuntut meningkatnya kualitas keamanan jaringan simak online. Terutama dengan semakin terbukanya pengetahuan hacking dan cracking, didukung dengan banyak nya tools yang tersedia dengan mudah dan kebanyakan free, semakin mempermudah para intruder dan attacker untuk melakukan aksi penyusupan ataupun serangan. Universitas Islam Negeri (UIN) Raden Fatah Palembang merupakan salah satu Perguruan Tinggi Islam Negeri yang berada di kota Palembang. UIN memiliki simak online yang terbagi menjadi sembilan bagian menurut fakultas masing-masing yaitu simak Simak Fak.USHPI, Simak Fak.Syariah, Simak Fak.Tarbiyah, Simak Fak.Adab, Simak Fak.Dakwah, Simak FEBI, Simak Pascasarjana, Simak Fak SAINSTEK, Simak Fak.Ilmu Sosial Dan Ilmu Politik yang berfungsi mengelola seputar sistem informasi mahasiswa seperti file mahasiswa, form nilai (KHS), penjadwalan, pengumuman atau informasi kampus dan sebagainya. Permasalahannya adalah simak online tersebut pernah mengalami serangan hacker pada bulan Mei 2016 dimana hacker menyusup pada bagian sistem akademik dengan mengubah tampilan halaman depan dan melakukan perubahan nilai serta saat diakses sering mengalami koneksi yang lambat serta terkadang koneksi yang terputus. Berdasarkan data diatas ternyata simak online Universitas Islam Negeri (UIN) Raden Fatah Palembang rentan terhadap penyusupan oleh karena itu penulis ingin melakukan penelitian untuk melakukan pengujian mengenai tingkat kerentanan simak online UIN Raden Fatah Palembang terhadap penyusup.

Hijacking Session merupakan aksi pengambilan kendali session milik user lain setelah sebelumnya "pembajak" berhasil memperoleh autentifikasi ID session yang biasanya tersimpan dalam cookies atau suatu kegiatan yang berusaha untuk memasuki (menyusup) ke dalam sistem

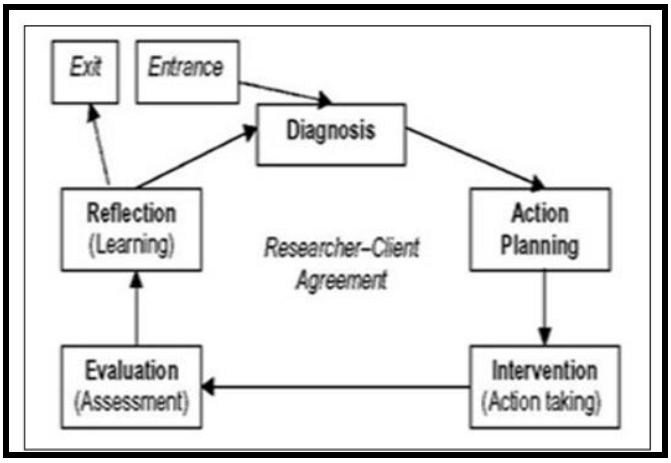
melalui sistem operasional lainnya yang dijalankan oleh seseorang. Sistem ini dapat berupa server, jaringan/networking (LAN/WAN), situs web, software atau bahkan kombinasi dari beberapa sistem tersebut.[3]

2. METODE PENELITIAN

A. *Metode Action Research*

Metode penelitian yang akan digunakan adalah metode action research.) Metode Action Research merupakan penelitian tindakan. Metode action research penelitian yang bersifat partisipatif dan kolaboratif. Maksudnya penelitiannya dilakukan sendiri oleh peneliti, dengan penelitian tindakan. [1] Action research dibagi dalam beberapa tahapan yang merupakan siklus, yaitu:

a. Tahap Pertama (*Diagnosing*)
   Mengidentifikasi permasalahan keamanan pada Sistem Informasi Akademik (Simak) Online yang terkait langsung mengenai masalah-masalah yang dihadapi UIN Raden Fatah Palembang.
b. Tahap Kedua (*Action Planning*)
   Memahami pokok masalah yang ada kemudian dilanjutkan dengan menyusun rencana tindakan yang tepat untuk menyelesaikan masalah yang ada dengan menyiapkan kebutuhan perangkat hardware dan software.
c. Tahap Ketiga (*Action Taking*)
   Melakukan mengujian Hijacking Session atau penyusupan dengan menggunakan tools ettercap (OS Kali Linux) dengan harapan dapat menyelesaikan masalah. Selanjutnya dengan model dibuat berdasarkan sketsa infrastruktur jaringan yang telah ditentukan.
d. Tahap Keempat (*Evaluating*)
   Setelah melakukan tahapan pengujian, proses selanjutnya melakukan analisis dan evaluasi hasil yang didapat dengan menggunakan aplikasi Wiresharks sehingga dapat diketahui kelebihan dan kelemahan sistem simak online yang telah berjalan.
e. Tahap Kelima (*Learning / Reflecting*)
   Setelah semuanya selesai, maka tahap akhir adalah melaksanakan review dan evaluasi tahap demi tahap kemudian penelitian ini dapat berakhir. Hasilnya juga mempertimbangkan untuk tindakan kedepan.



Gambar 1. *Action Research Model*.

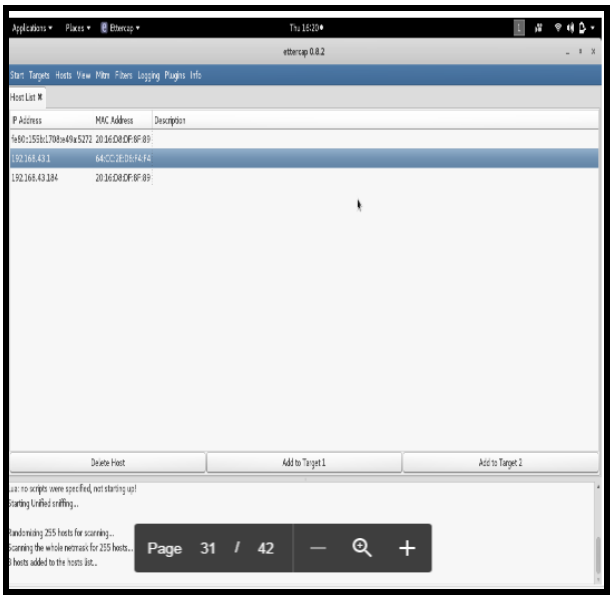
3. HASIL DAN PEMBAHASAN

Address Resolution Protocol (ARP) adalah sebuah protokol dalam TCP/IP Protocol yang digunakan untuk melakukan resolusi alamat IP ke dalam alamat *Media Access Control* (MAC Address). Ketika sebuah komputer mencoba untuk mengakses komputer lain dengan menggunakan alamat IP, maka alamat IP yang dimiliki oleh komputer yang dituju harus diterjemahkan terlebih dahulu ke dalam MAC Address agar frame-frame data dapat diteruskan ke tujuan dan diletakkan di atas media transmisi, setelah diproses terlebih dahulu oleh *Network Interface Card* (NIC). Metode ARP Spoofing merupakan konsep serangan penyadapan atau penyusupan diantara dua mesin yang sedang berkomunikasi atau biasa disebut Man In the Middle Attack.[5][6]

Untuk pengujian penyadapan atau penyusupan (Hijacking Session) terhadap session Sistem Informasi Akademik (Simak) online Universitas Islam Negeri (UIN) Raden Fatah penulis mengunakan software sniffing yang cukup terkenal yaitu software ettercap pada komputer penyusup (sniffer), dimana ettercap merupakan aplikasi yang terdapat pada sistem operasi hacking Kali Linux. Pengujian menggunakan interface wlan0 / interface card wireless pada komputer penyusup yang terhubung pada access point. Pada saat scan terdapat IP address dan mac address Access Point(Target 1) dan Client (Target 2), IP address Access Point yaitu 192.168.43.1 dengan mac address yaitu 64:CC:2E:D6:F4:F4 sedangkan IP address web Client 192.168.43.184 dengan mac address yaitu 20:16:D8:DF:8F:89 .

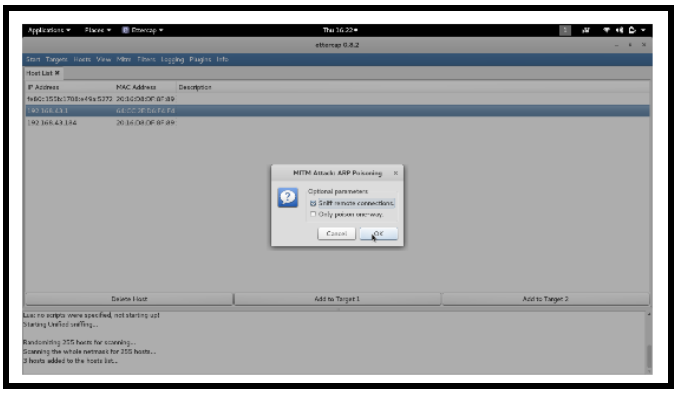
TABEL 1. IP Address dan Mac Address

No	Posisi	IP Address	Mac Address
1	Penyusup	192.168.43.129	80:A5:89:6F:32:1D
2	Gateway/AP	192.168.43.1	64:CC:2E:D6:F4:F4
3	Client	192.168.43.184	20:16:D8:DF:8F:89



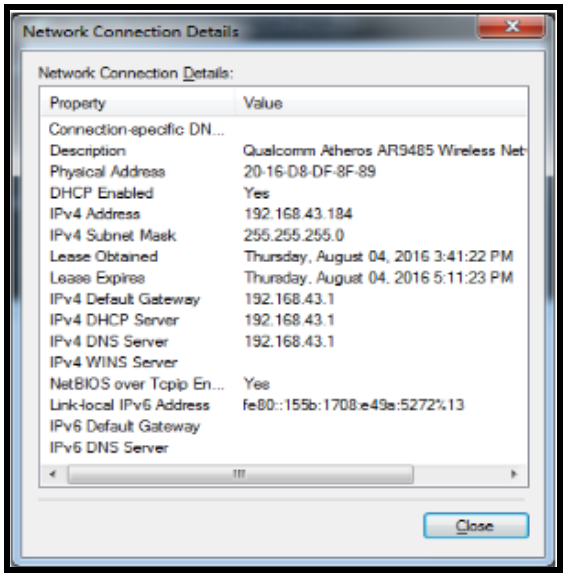
Gambar 2. Scan Host dan hasil scanning

4. Jalankan sniff remote connection kemudian pilih ok setelah itu klik start sniffing untuk memulai penyusupan dilihat pada gambar 2.



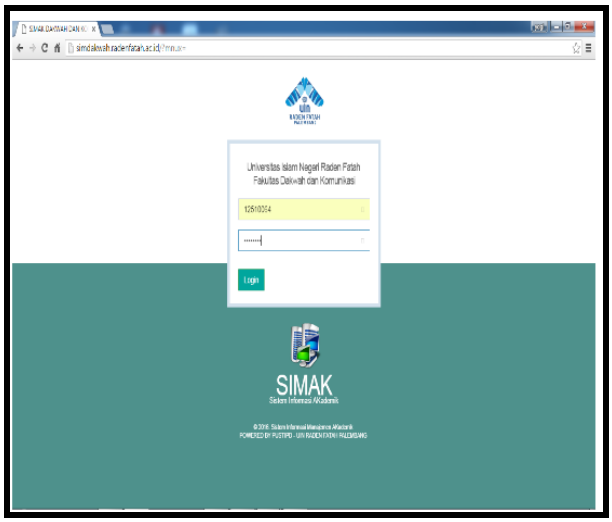
Gambar 3. Proses penyusupan simak online

Pada komputer client diperoleh IP Address Wifi melalui DHCP Server yaitu 192.168.43.184 dengan mac address 20:16:D8:DF:8F:89, IP Address dan Mac address tersebut akan tampil pada aplikasi ettercap seperti pada gambar 4.



Gambar 4. IP Address Client dan Mac Address

Hasil tampilan login Sistem Informasi Akademik (Simak) online Universitas Islam Negeri (UIN) Raden Fatah yang diakses dari komputer client dengan menggunakan browser GoogleChrome, saat komputer penyusup sedang aktif, secara bersamaan client akan mencoba login menggunakan user dan password mahasiswa.



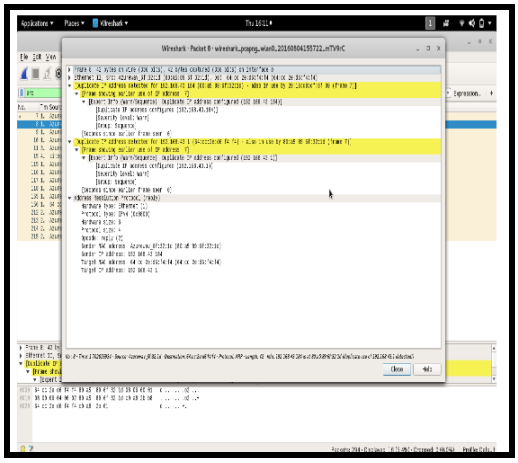
Gambar 5. Login User dan Password Simak

Dari hasil pengujian diperoleh hasil dimana penyusup atau hacker dengan IP Address 192.168.43.219 dapat mengamati user login yang digunakan Client saat terkoneksi ke Sistem Informasi Akademik (Simak) online UIN Raden Fatah pada fakultas dakwah yaitu http://simdakwah.radenfatah.ac.id dan penyusup juga bisa memperoleh password login dari user tersebut, dimana user yang diperoleh yaitu 12510064 dan password 12510064. hal ini dikarenakan sistem sekuriti atau keamanan sistem Informasi Akademik (Simak) online Universitas Islam Negeri (UIN) Raden Fatah tidak menggunakan proses enkripsi pada password login sehingga sangat mudah diamati oleh penyusup.

Gambar 6. Hasil penyusupan Simak Server

Aplikasi yang digunakan untuk menganalisis jaringan menggunakan Wire Shark. WireShark merupakan tool yang ditujukan untuk penganalisisan paket data jaringan. Tujuan dari monitoring dengan wireshark adalah Memecahkan masalah jaringan, Memeriksa Keamanan Jaringan, Men-debug implementasi protocol dan mempelajari protocol jaringan internal. [2][3]
Pada gambar dibawah ini terlihat Mac-address access point yang semula 64:CC:2E:D6:F4:F4 berubah menjadi mac address penyusup yaitu 80:A5:89:6F:32:1D, dengan menggunakan tool

wireshark terlihat terjadi duplikasi (duplicate) mac-address access point / Wifi yang berubah menjadi mac-address penyusup sehingga paket yang menuju ke server akan bisa diamati melalui software wireshark melalui penyusup.



Gambar 7. Hasil pengamatan wireshark

Dengan menggunakan user dan password login saat melakukan membuka Sistem Informasi Akademik (Simak) online Universitas Islam Negeri (UIN) Raden Fatah, sangat rentan terhadap penyusup yang ingin mencoba mengakses web server, dengan menggunakan software wireshark dengan mudah dapat mengamati proses dan mengetahui informasi apa saja yang diakses antara server dan client remote yang tentunya sangat berbahaya bagi keamanan sistem Sistem Informasi Akademik (Simak) online Universitas Islam Negeri (UIN) Raden Fatah. Untuk mengatasi permasalahan tersebut salah satu solusi adalah menerapkan sistem keamanan enkripsi pada web simak online dengan menggunakan teknologi keamanan SSL atau *Secure Sockets Layer* . SSL atau *Secure Sockets* Layer adalah sebuah protokol keamanan data yang digunakan untuk menjaga pengiriman data web server dan pengguna situs web tersebut.
Untuk mengaktifkan SSL pada situs simak online, hanya perlu memasang sertifikat SSL yang sesuai dengan server dan situs. Setelah SSL terpasang, user bisa mengakses situs secara aman dengan mengganti URL yang sebelumnya http:// menjadi https://. Hal ini dapat terlihat dari indikator atau ikon gembok pada browser atau juga alamat situs yang diakses diindikasikan dengan warna hijau pada baris alamat browser.

5. KESIMPULAN

ARP Spoofing adalah sebuah teknik penyadapan oleh pihak ketiga yang dilakukan dalam sebuah jaringan LAN maupun internet. Dengan metode tersebut, attacker dapat menyadap transmisi, modifikasi trafik, hingga menghentikan trafik komunikasi antar dua mesin yang terhubung dalam satu jaringan lokal (LAN) maupun jaringan internet melalui Wifi.
Web Sistem Informasi Akademik (Simak) online Universitas Islam Negeri (UIN) Raden Fatah sangat rentan terhadap serangan ARP Spoofing, hal ini dibuktikan saat pengujian dimana user account dan password dapat dilihat pada saat menggunakan aplikasi ettercap

REFERENSI

[1] Kock, Ned. 2007. Information systems Action Research An Applied View Of emerging Concepts and Methods. Texas A & M International University. USA

[2] Kurniawan,Agus. 2012. Network Forensics (Panduan Analisis dan Investigasi Paket Data Jaringan menggunakan Wireshark). Yogyakarta :Andi Offset

[3]Anhar. 2010. PHP & MySql Secara Otodidak. Jakarta: PT TransMedia

[4] Sugiantoro, Bambang & Istianto, Jazi (Seminar Nasional Informatika 2 Mei 2010). Analisa sistem keamanan Intrusion Detection System (IDS), Firewall System, Database System dan Monitoring System menggunakan Agent bergerak.

[5] Sumit Miglani & Indeerjeet Kaur. 2013. "Feasibility analysis of different methods for prevention against ARP Spoofing". International Journal Of Scientific and Research Publications. Vol 3 2013. ISSN 2250-315

[6] Ariyus, Dony (2006). *Computer Security*. Yogyakarta: Penerbit ANDI.