ISBN: 978-623-7297-02-4

PEMANFAATAN BETTERCAP SEBAGAI TEKNIK SNIFFING PADA PAKET TRAFIK JARINGAN WIFI

Dian Kurnia
Fakultas Sains dan Teknologi, Univeristas Pembangunan Panca Budi
email: diankurnia68@dosen.pancabudi.ac.id

Abstrak

Perancangan topologi jaringan yang aman merupakan solusi untuk mengamankan server sebuah instansi. Serangan hacker yang kerap sekali mencari kesempatan untuk mengetahui aktivitas suatu jaringan, dan mencari celah kelemahan yang ada. Teknik dengan kemampuan dalam merecord semua kegiatan paket masuk dan keluar pada suatu data dan mencari intersep yang memungkinkan merecord username dan password ketika host login pada suatu ur, dalam hal ini pada segmen jaringan antara host dan hacker disebut Teknik Sniffing. Pada penelitian ini penulis menggunakan teknik sniffing untuk mengetahui kelemahan dari jaringan wifi dan LAN di Universitas Pembangunan Panca Budi Medan. Dari hasil penelitian beberapa host yang menjadi target sniffing, diketahui mengakses beberapa url sosisal media dan page login url lainnya. Akses username dan password di record ketika aplikasi bettercap melakukan fitur sniffer disetiap hostnya. Ada beberapa host yang dijadikan target hanya akan tetapi username dan password tidak ditemukan oleh bettercap hal ini dikarenakan host yang menjadi target mengaktifkan firewall dan memiliki anti virus security berbayar yang update.

Kata-Kata Kunci: *Sniffing, Bettercap, Wifi, Ubuntu*

I. PENDAHULUAN

Analisis jaringan bisa juga dikatakan sebagai upaya-upaya analisis seseorang dalam menganalisis suatu jaringan. Analisis jaringan ini dapat berupa analisis trafik, protocol, sniffing, penyadapan dan sebagainya.[1] Persoalan yang sering terjadi ketika komputer mengalami tidak dapat meng*share* folder pada jaringan, brainware tidak dapat mengakses email dan juga jaringan terjadi *delay* dalam transmisikan data. Persoalan tersebut bisa saja muncul karena adanya serangan di jaringan yang diawali adanya suatu upaya *attaker* mendapatkan *access control* pada suatu jaringan. *Access control* ini dapat diakses jika *attacker* mendapatkan login suatu *username* dan *password* pada suatu sistem jaringan dalam hal ini berhubungan dengan autentikasi akses. Penelitian sebelumnya Rupam (2013) melakukan peninjauan teoritis secara detail mengenai bagaimana mendeteksi paket menggunakan paket *sniffing.*[2] Penelitian selanjutnya, sutarti (2017), membangun *honeyspo*t pada jaringan nirkabel kemudian menganalisisnya dengan melakukan teknik serangan DDOS pada jaringan *honeyspot* yang di bangun.[3]

Dalam penelitian ini peneliti merancang suatu jaringan wifi public yang terhubung ke internet melalui modem. Jaringan yang telah dibangun dilakukan analisis trafik jaringan, protocol jaringan dengan teknik-tenik *sniffing*. Teknik *sniffing* adalah teknik yang fokus dalam memantau atau mengindentifikasi paket-paket data yang keluar masuk pada jaringan tertentu. Teknik – teknik *sniffing* ini akan diurutkan sesuai dengan tahapan penyerangannya dengan melakukan pengujian dan perbedaan tahapan. Tahapan-tahapan penyerangan dengan hasil yang mangkus akan di pilih dan dijadikan model penyerangan yang tepat nantinya dalam menganalisis trafik data yang berjalan pada tipe topologi jaringan private tersebut. *Sniffing* akan difokuskan pada pencarian username dan password untuk login web dan mencoba mengetahui lebih paket data yang keluar masuk ketika seorang user login pada *page login web* dan keseluruhan aktifitas user dalam mengakses url di browser.

Sniffing merupakan proses pengendusan paket data pada sistem jaringan komputer, yang diantaranya dapat memonitor dan menangkap semua lalu lintas jaringan yang lewat tanpa peduli kepada siapa paket itu di kirimkan. Contoh dampak negatif *sniffing*, seseorang dapat melihat paket data informasi seperti *username* dan *password* yang lewat pada jaringan komputer. Contoh dampak positif *sniffing*. Seorang admin dapat menganalisa paket-paket data yang lewat pada jaringan untuk keperluan optimasi jaringan, seperti dengan melakukan penganalisaan paket data, dapat diketahui dapat membahayakan performa jaringan atau tidak, dan dapat mengetahui adanya penyusup atau tidak. Bahaya yang mengancam dari proses *sniffing* yaitu hilangnya sifat *privacy* dan *confidentiality* seperti tercurinya informasi penting dan rahasia seperti *username* dan *password*.[4]

Salah satu software sniffing yang salah satunya chain & ebel yang versi terbaru dapat memonitor otentikasi routing protokol dan ,kamus dan brute-force cracker untuk semua algoritma hashing umum dan untuk otentikasi spesifik, kalkulator password/hash, serangan kriptanalisis, dekoder password dan beberapa utilitas tidak begitu umum yang terkait dengan jaringan dan sistem keamanan.[5]

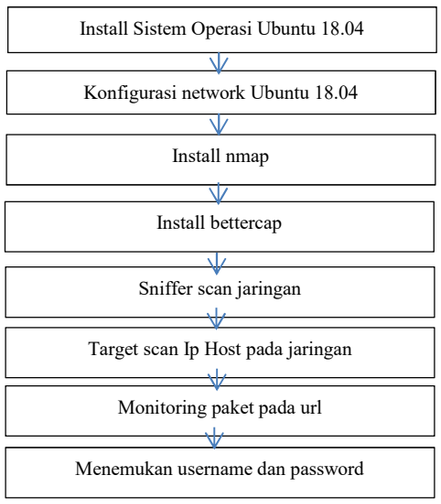
Bettercap termasuk software dengan kategori open source dan tool keamanan jaringan untuk serangan *Man-In-The-Middle*, aplikasi tersebut hanya berjalan pada jaringan LAN dengan kerja menganalisis suatu jaringan protocol computer dan menngumpulkan infotmasi paket yang dikirim dan di terima oleh computer. Teknik bettercap melakukan Intersep pada jaringan dan mengubah trafik pada sebuah segmen jaringan, menangkap password pada IP Host Target. Melakukan

pengubahan script dengan kemampuan penuh dari fitur bettercap. Penyadapan aktif terhadap sejumlah protocol umum seperti TELNET, FTP, POP, IMAP, rlogin, SSH1, ICQ, SMB, MySQL, HTTP, NNTP, X11, Napster, IRC, RIP, BGP, SOCKS 5, IMAP 4, VNC, LDAP, NFS, SNMP, Half-Life, Quake 3, MSN, YMSG![7]

Sistem operasi adalah sekumpulan rutin perangkat lunak yang berada diantara program aplikasi dan perangkat keras. Sistem operasi memiliki tugas yaitu mengelola seluruh sumber daya sistem komputer dan sebagai penyedia layanan. Sistem operasi menyediakan System Call (berupa fungsi-fungsi atau API=Application Programming Interface). System Call ini memberikan abstraksi tingkat tinggi mesin untuk pemrograman.[8]

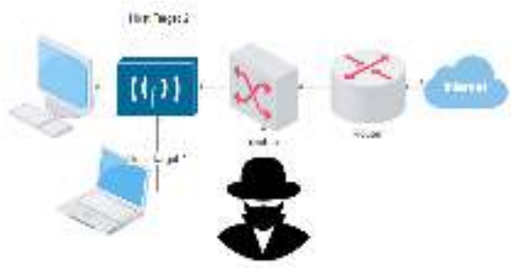
II. METODE PENELITIAN

Pada penelitian ini, penulis melakukan tahapan-tahapan penelitian. Adapun tahapan penelitian yang dilakukan sebagai berikut :



Perintah linux yang digunakan untuk menyelesaikan tahapan-tahapan instalasi tersebut adalah

```
# apt-get update
#apt-get install nmap
#apt-get install bettercap
#bettercap --sniffer
#bettercap -T TARGET_IP --proxy -P
POST
```



Gambar 1. Topologi jaringan yang dianalisis

Adapun topologi jaringan yang dianalisis oleh penulis yaitu pada jaringan internet di Universitas Pembangunan Panca Budi Medan. Internet yang bersumber dari ruang BPSI kemudian didistribusikan melalui router mikrotik dan pada mikrotik disetting hotspot yang terintegrasi username dan password login pada server linux centos di ruangan BPSI Universitas Pembangunan Panca Budi.

Adapun bahan alat yang digunakan dalam menganalisa paket data menggunakan Bettercap

Kebutuhan perangkat lunak yang digunakan sebagai berikut ;

a. Sistem Operasi Linux Ubuntu 18.04
   System operasi ini digunakan dikarenakan system yang terupdate untuk fitur bettercap.
b. Nmap
   aplikasi dengan bekerja berfokus pada scanning port di setiap perangkat jaringan.
c. Bettercap
   Aplikasi dan merupakan fitur dari linux Ubuntu 18.04, dengan melakukan scanning paket data yang masuk dan keluar pada jaringan wifi atau LAN keselurahan, ataupun melakukan scanning pada IP Address/host tertentu.

Kebutuhan perangkat keras yang digunakan oleh peneliti dalam menganalisa perangkat jaringan LAN dan Wifi yaitu:

a. Processor Core i3 2.13 Ghz
b. RAM 4 GB
c. Hardisk 320 GB
d. Wifi Realtek RTL8191SE Wireless LAN 802.11n PCI-E NIC On Board

III. HASIL DAN PEMBAHASAN

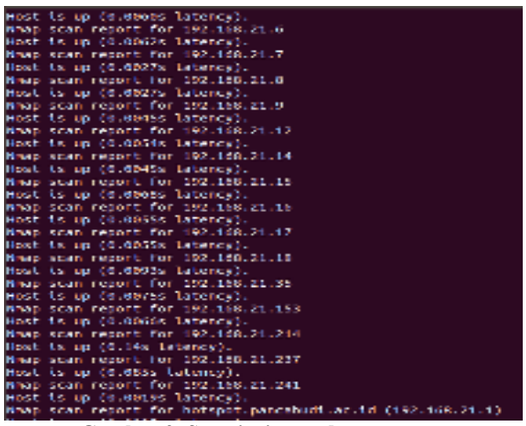
Pengujian paket trafik ketika user melakukan pengaksesan internet melalui koneksi jaringan wifi public, Dengan menggunakan Bettercap pada Sistem Operasi Ubuntu 18.04. dilakukan teknik sniffing untuk mendapatkan username dan password page login web dari kegiatan user aktif mengakses url seperti media social, email dan lain-lain. Adapun hasil yang di dapat dari teknik sniffing sebagai berikut ;

Tabel 1. Hasil sniffing dengan Bettercap

No	Target IP/Host	Url	username	password
1	192.168.21.6	www.gmail.com	desaignbagus@gmail.com	Lupa1979bagus
2	192.168.21.7	www.yahoo.com	brainjaya@yahoo.com	Brainkontak
3	192.168.21.8	www.medanloker.com	cobalamar@gmail.com	ADM##2019
4	192.168.21.9	www.facebook.com	Anita.medan@gmail.com	Nita@@17
5	192.168.21.12	www.twitter.com	Ana_gaul1995@gmail.com	pastiAnakgaul
6	192.168.21.14	www.instagram.com	Medan_1990@gmail.com	Liketoba1990
7	192.168.21.15	www.olx.com	-	-
8	192.168.21.16	https://dosen.pancabudi.ac.id/	-	-

Dari hasil sniffing diketahui ada beberapa login url tidak dapat diketahui username dan password, hal ini dimungkinan target host yang disniffing mengaktifkan firewall pada system operasinya dan menginstall aplikasi anti virus seperti kapersky, AVG security dan Avast Security yang terlisensi bayar resmi kepada penyedia aplikasi anti virus tersebut.

Tahapan awal yaitu menscan jaringan wifi hotspot pancabudi dengan menggunakan nmap yang ada di fitur Ubuntu 18.04.



Gambar 2. Scan jaringan dengan map

Kemudian dilakukan proses --sniffer untuk mencari kemungkinan peluang paket trafik yang terindentifikasi username dan password ketika user mengakses beberapa page login.

Gambar 3. Proses sniffer pada bettercap

Tampilan berikutnya mendapatkan beberapa paket data yang memuat autentikasi ketika login

Gambar 4. Proses pengumpulan paket data berupa code Hash

Teknik berikutnya menscan semua network dengan list url yang diakses setiap host yang aktif pada jaringan hotspot Universitas Pembangunan Panca Budi

Gambar 5. Scan setiap url yang diakses oleh user

IV. KESIMPULAN

Dari hasil pengujian dan pembahasan yang telah dilakukan diketahui bettercap dapat berjalan pada protocol http dan https, bettercap dengan mudah menangkap paket-paket yang berjalan pada host yang kondisi firewall dalam keadaaan non aktif. Pada topologi jaringan yang lebih kompleks seperti pada hotspot mikrotik yang memiliki lisensi level 6 proses penetrasi dan sniffing menggunakan bettercap kurang mangkus dalam mendapatkan username dan password.

DAFTAR PUSTAKA

[1] W. Uses, N. Analysis, D. Sniffers, P. A. Sniffers, and N. Analysis, Chapter 1 *Introducing Network Analysis*.

[2] A. Verma and A. Singh, 2013, *An Approach to Detect Packets Using Packet Sniffing*, vol. 4, no. 3, pp. 21–33.

[3] P. Studi *et al.*, 2017, *Perancangan Dan Analisis Keamanan Jaringan Nirkabel Dari Serangan Ddos (Distributed Denial Of Service) Berbasis Honeypot*, vol. 4, no. 2.

[4] M. F. Adriant, 2015, *Implementasi Wireshark Untuk Penyadapan (Sniffing) Paket Data Jaringan*, *Semin. Nas. Cendekiawan*, pp. 224–228.

[5] K. E. Pramudita, 2011, *Brute Force Attack dan Penerapannya pada Password Cracking*, no. 2011, p. 6.

[6] M. J. Syahputra *et al.*, Deteksi Serangan Pada Jaringan Komputer Dengan Wireshark.

[7] Group, : Linh, Manish, Mario, and Mei, Man-In-The-Middle Attack Using Ettercap.

[8] J. Handoyo, 2918, Kajian Penggunaan Mikrotik Router Ostm Sebagai Router Pada Jaringan Komputer, *J. Transform.*, vol. 9, no. 1, p. 20.