BAB II

TINJAUAN PUSTAKA

A. Hasil Penelitian Terdahulu

1. (Jamaludin & Suaeb, 2018) melakukan penelitian mengenai perkembangan teknologi informasi khususnya di bidang jaringan komputer memungkinkan pertukaran informasi lebih cepat dan lebih kompleks dan data yang dipertukarkan dapat bervariasi. Pengguna internet dan penyedia jaringan nirkabel internet, memungkinkan mengakses apapun termasuk website dari manapun mereka mau, yang menyebabkan isu keamanan informasi menjadi penting. Proses penyadapan informasi (Sniffing) pada jaringan komputer menjadi semakin biasa dilakukan, baik untuk kegunaan yang bersifat positif maupun yang bersifat sebaliknya. Penelitian ini memberikan gambaran umum tentang keamanan website Simak Unismuh terhadap proses sniffing pada jaringan nirkabel, serta gambaran umum tentang kemungkinan metode serangan yang dapat terjadi pada website Simak Unismuh. Penelitian ini juga memberikan solusi kepada pengguna internet dan web developer untuk mencegah serangan dari kerentanan yang ditemukan. Dalam penelitian ini dilakukan dua tahap, yang pertama yaitu mengidentifikasi tingkat keamanan website Simak Unismuh menggunakan aplikasi Wireshark dan yang kedua yaitu membandingkan tingkat keamanan website Simak Unismuh dengan Google Account untuk mengetahui kelemahannya. Hasil dari penelitian ini adalah dengan penyerangan packet sniffing pada website Simak Unismuh, dapat merekam dan menampilkan informasi sensitif seperti username dan password dengan menggunakan aplikasi wireshark. Selain itu website Simak Unismuh

rentan terhadap serangan MITM (man in the middle), karena belum menggunakan sertifikat SSL

2. (Siregar, 2019) telah melakukan pengujian tentang keamanan jaringan wifi yang sangat dibutuhkan untuk menjaga data serta menjamin ketersediaan layanan bagi penggunanya agar terhindar dari serangan yang sering terjadi seperti sniffing dan lainnya. Pengujian keamanan secara berkala terhadap sistem sangatlah penting agar dapat mengetahui celah-celah mana yang terbuka. Pengujian analisis dari keamanan wifi digunakan ettercap sebagai tools yang akan menganalisis dari keamanan wifi dan juga sebagai media untuk melakukan penetrasi pengujian pada wifi tersebut. Karena penggunaan fasilitas wifi telah menjadi kebutuhan bagi setiap perusahaan, dimana dengan wifi para karyawan bisa langsung menghubungakan koneksi ke internet untuk kebutuhan transfer data atau lainnya.
3. (Aufan et al., 2012) telah melakukan analisis keamanan website Universitas XYZ yang melakukan pertukaran informasi melalui sistem berbasis web. Mengingat website ini dapat diakses secara luas, maka dinilai perlu memperhatikan keamanan website. Terdapat beberapa cara yang dapat digunakan untuk melakukan pengujian terhadap kemanan website. Salah satunya adalah dengan melakukan Web Penetration Testing. Alasan dilakukannya penelitian ini adalah karena peneliti mendengar dari beberapa sumber baik dosen maupun temen mahasiswa, bahwa sistem informasi akademik yang dimiliki oleh Universitas XYZ tidaklah aman atau dapat di hacking atau dijebol sewaktu – waktu. Alasan lain mengapa dilakukannya penelitian ini adalah untuk mengetahui pula seberapa tingginya tingkat keamanan sistem informasi akademik yang ada di Universitas XYZ. Dari penelitian diatas, peneliti dapat menarik

kesimpulan bahwa untuk jenis serangan sql injection yang dilakukan terhadap target yaitu sistem informasi akademik Universitas XYZ, sistem tersebut telah AMAN. Perlu digaris bawahi kembali peneliti dapat menyimpulkan sistem telah aman HANYA UNTUK JENIS SERANGAN SQL INJECTION. Untuk jenis serangan yang lainnya, peneliti dapat menyimpulkan bahwa sistem target BELUM AMAN.

4. (Fauzi & Suartana, 2018) telah melakukan penelitian yang membahas pendeteksi serangan packet sniffing pada fasilitas access point dengan menggunakan sistem IDS. Intrusion Detection System (IDS) adalah sebuah sistem yang melakukan pengawasan terhadap traffic jaringan dan pengawasan terhadap kegiatan-kegiatan yang mencurigakan didalam sebuah sistem jaringan. Pada saat melakukan simulasi serangan packet sniffing dengan indikasi arp spoof menggukan tools ettercap. Pada protokol HTTP, tools ettercap mampu merekam aktivitas jaringan internet dan mampu menangkap user dan password pada saat melakukan login pada protokol HTTP, pada protokol HTTPS tidak dapat melakukan aktivitas internet karena protokol HTTPS memiliki security. Pada saat IDS snort dijalankan, maka IDS akan memonitoring jaringan internet yang sedang terhubung. Ketika menemukan kegiatan-kegiatan yang mencurigakan terutama sebuah serangan packet sniffing dengan indikasi arp spoofing, maka IDS akan memberikan alert berupa text “Overwrite Attack” pada PC yang sudah terinstall IDS.
5. (Susanto et al., 2018) telah melakukan analisis sniffing password menggunakan aplikasi cain dan abel pada jaringan wifi universitas semarang. Data dikirim melewati beberapa terminal untuk sampai tujuan berarti akan memberikan kesempatan pada user lain yang tidak bertanggung jawab untuk menyadap atau mengubah data, bahkan

sampai mencuri data tersebut. Khususnya ancaman serangan dari sniffing. Aktivitas sniffing, yaitu penyadapan data dijaringan komputer dengan cara membelokkan data, merupakan aktivitas yang mudah dilakukan oleh para hacker. Aktivitas ini biasanya disalah gunakan oleh orang yang tidak bertanggung jawab untuk mencuri informasi penting dari korbannya. Hal demikian terjadi karena kurang adanya pengamanan yang tepat maupun ketidak tahuan masyarakat awam. penggunaan Aplikasi Cain and Abel, yang digunakan untuk mengintai lalu lintas pada jaringan wifi USM, aplikasi Cain and Abel ini melakukan sniffing yang merekam seluruh aktivitas yang terjadi pada jaringan.

6. (Hasanah & Latiffani, 2020) telah melakukan penelitian kebocoran jaringan keamanan wifi meski sudah menggunakan metode WPA2 PSK yang tidak jarang masih sering terjadi sehingga orang yang tidak berhak dan bertanggung jawab dapat menggunakan jaringan hostpot. Kondisi ini perlu ditangani meningkatkan keamanan pada hostpot jaringan sehingga keamanan dan penggunaan hostpot bias lebih terkontrol.
7. (Pambudi & Bariyah, 2020) telah melakukan penelitian mengenai Sistem Absensi Siswa Menggunakan Wi-fi Direct Dan Wi-fi Hostpot. Dalam sistem kehadiran siswa, wifi memungkinkan fleksibilitas dan meminimalkan biaya sementara tetap menjaga keamanan dan validitas file proses verifikasi, prosesnya juga harus seperti semudah mungkin tanpa campur tangan pengguna, Serta untuk menghilangkan kebutuhan akan perangkat tambahan yang harus dipasang.

B. Landasan Teori

a. Keamanan Jaringan

Keamanan informasi adalah sekumpulan metodologi, praktik, ataupun proses yang dirancang dan diterapkan untuk melindungi informasi atau data pribadi dari akses, penggunaan, penyalahgunaan, gangguan, atau modifikasi yang tidak sah. Keamanan informasi bertujuan untuk melindungi data pada berbagai tahap, baik itu ketika proses menyimpan, mentransfer, atau menggunakannya.

Perusahaan akan mengembangkan kebijakan keamanan informasi untuk menangani dan melindungi info atau data penting yang mereka miliki. Kebijakan yang sudah dikembangkan tersebut akan berlaku untuk seluruh struktur IT.

Selain itu, kebijakan keamanan informasi juga berguna untuk menentukan siapa yang memiliki akses ke berbagai jenis data, bagaimana identitas akan diautentikasikan, metode apa yang dipergunakan untuk mengamankan informasi, dan lain-lain. Langkah-langkah tersebut akan membantu Anda mencegah bahaya akan pencurian, modifikasi, atau kehilangan informasi penting.

Perlu diketahui, bahwa sebagian besar kebijakan keamanan informasi akan memiliki fokus atau tujuan yang mengacu pada aspel CIA triad. Aspek tersebut yaitu confidentiality, integrity, dan availability. Setiap serangan di dunia maya pada umumnya akan mencoba melanggar setidaknya salah satu aspek atau atribut dalam CIA triad.

Dengan memiliki pemahaman yang baik tentang model keamanan informasi ini, Anda akan lebih terbantu untuk meminimalisir risiko serangan atau kesalahan sistem

dengan lebih baik. Dengan kebijakan keamanan yang tepat, Anda dapat melindungi informasi penting dari aktivitas-aktivitas yang tidak sah.

Aspek-aspek dalam keamanan informasi :

1. Confidentiality (Kerahasiaan)

   Ketika kita membahas mengenai aspek confidentiality atau kerahasiaan informasi, maka kita sedang berbicara mengenai serangkaian upaya perlindungan agar informasi tidak terakses oleh pihak yang tidak berwenang.

   Informasi rahasia memang dianggap sebagai data yang bernilai oleh para cyber hacker. Informasi yang diincar biasanya berupa informasi pelanggan, data karyawan, kekayaan intelektual, atau informasi mengenai rahasia dagang. Oleh karena itulah para cyber hacker terus mencari kerentanan yang ada pada dalam sistem agar mereka bisa mengakses info-info penting tersebut.

   Pada umumnya, informasi rahasia dapat jatuh ke tangan yang salah karena data breach atau ancaman orang dalam. Beberapa jenis serangan yang umum digunakan untuk mengakses informasi rahasia tersebut seperti :

   - Serangan Man in The Middle
   - Pembobolan enkripsi
   - Serangan eavesdropping

Untuk melindunginya, terdapat sejumlah langkah yang dapat dipergunakan seperti dengan menerapkan autentikasi dua faktor, penggunaan password yang kuat, enkripsi, dan lain-lain.

Meskipun demikian, Anda juga perlu memahami bahwa informasi rahasia juga dapat terakses oleh pihak yang tidak sah karena kecerobohan atau kesalahan pengguna, serta kontrol keamanan yang tidak memadai. Contohnya seperti penggunaan password yang lemah, berbagi akun, atau karena social engineering karena security awareness yang kurang.

Oleh karena itulah, pelatihan karyawan atau user juga dapat dilakukan sebagai langkah pencegahan tambahan agar informasi rahasia bisa tetap terlindungi dengan baik. Jadi, kesimpulannya aspek confidentiality ini memiliki tujuan untuk melindungi informasi dari akses dan penyalahgunaan info yang tidak sah.

2. Integrity

Dalam keamanan informasi, integrity atau integritas mengacu pada suatu metode atau langkah-langkah untuk menjaga agar data atau informasi tidak dapat dimanipulasi, diubah atau diedit oleh pihak yang tidak punya wewenang. Langkah-langkah ini memberikan jaminan atas keakuratan dan kelengkapan informasi.

Seperti halnya dengan perlindungan informasi rahasia, perlindungan integritas juga perlu untuk dilakukan. Bayangkan jika Anda memiliki sebuah web e-commerce yang diretas oleh hacker sehingga mereka dapat mengubah harga produk Anda menjadi

jauh lebih murah. Contoh lain dari kegagalan perlindungan integritas seperti ketika pengguna website mengunjungi halaman web Anda namun peretas mampu mengalihkan traffic tersebut ke website palsu. Serangan-serangan tersebut tentu akan membawa kerugian besar untuk perusahaan Anda.

Perlu Anda ketahui, aspek perlindungan integrity tidak hanya akan melindungi keakuratan informasi dari serangan hacker namun juga untuk mencegah perubahan informasi yang tidak disengaja. Contohnya seperti kesalahan pengguna atau kerusakan sistem.

Untuk mencegah modifikasi informasi yang tidak diinginkan atau untuk memastikan bahwa informasi dapat dipulihkan kembali jika diubah oleh pihak tidak sah, maka terdapat beberapa langkah pencegahan yang bisa Anda lakukan. Beberapa diantaranya seperti :

- mengontrol akses pengguna
- enkripsi
- autentikasi yang ketat
- prosedur backup dan recovery
- version controls
- input validation

3. Availability

Aspek ketiga dalam CIA triad adalah availability atau ketersediaan. Artinya, dalam konteks keamanan informasi upaya untuk menjaga agar sebuah sistem tetap bisa digunakan adalah hal penting yang perlu dilakukan. Dengan memberikan perlindungan availability, Anda harus bisa memberikan jaminan bahwa sistem dan data dapat diakses oleh pengguna yang diautentikasi kapanpun informasi tersebut dibutuhkan.

Kelangsungan sebuah bisnis akan sangat bergantung pada pemeliharaan performa perangkat keras, perangkat lunak, dan saluran komunikasi yang digunakan untuk menyimpan dan memproses informasi. Ketika sebuah situs website perusahaan terganggu dan tidak dapat diakses, maka perusahaan dapat kehilangan banyak pendapatan. Selain itu pelanggan juga akan merasa tidak puas dengan performa web sehingga mempengaruhi reputasi perusahaan.

Para peretas biasanya mengganggu availability website menggunakan beberapa jenis serangan salah satunya adalah DDOS attack. Serangan tersebut dilakukan dengan cara membanjiri lalu lintas server, jaringan, atau sistem untuk mengganggu lalu lintas normal. Jika peretas berhasil melakukannya maka akses website dapat menghilang atau bekerja dengan sangat lambat.

Selain itu ketidaktersediaan informasi juga dapat terjadi karena beberapa hal lain seperti karena menggunakan bandwidth yang tidak mencukupi atau karena adanya kode berbahaya di dalam sistem.

Untuk menjaga aspek availability ini, terdapat beberapa upaya yang bisa Anda lakukan. Beberapa diantaranya seperti:

- menggunakan layanan pelindung DDoS
- menggunakan redundancy, firewall, dan proxy servers
- memastikan bahwa bandwidths yang digunakan mencukupi
- penggunaan access controls.

b. Aspek - Aspek Keamanan Jaringan

1. Privacy/Confidentiality

   Usaha untuk menjaga informasi dari orang yang tidak berhak mengakses. Privacy lebih kearah data-data yang sifatnya privat sedangkan confidentiality biasanya berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu (misalnya sebagai bagian dari pendaftaran sebuah servis) dan hanya diperbolehkan untuk keperluan tertentu tersebut.

   Contoh ancaman :

   - (Privacy) Email anggota tidak boleh dibaca oleh administrator server
   - (Confidentiality) Data pelanggan sebuah ISP dijaga kerahasiaannya

   Solusi :

   Kriptografi (enkripsi dan dekripsi)

2. Integrity

   Aspek ini menekankan bahwa informasi tidak boleh diubah tanpa seijin pemilik informasi.

   Contoh ancaman :

- Trojan, virus, man in the middle attack
- Pengubahan isi email

Solusi :

- Enkripsi
- Digital Signature

3. Availability

Aspek availability / ketersediaan berhubungan dengan ketersediaan informasi ketika dibutuhkan. System informasi yang diserang / dijebol dapat menghambat / meniadakan akses ke informasi.

Contoh hambatan :

- "Denial of Service attack" (DoS attack), dimana server dikirimi permintaan (biasanya palsu) yang bertubi-tubi atau permintaan yang diluar perkiraan sehingga tidak dapat melayani permintaan lain atau bahkan sampai down, hang, crash.
- Mailbomb, dimana seorang pemakai dikirimi email bertubi-tubi (katakan ribuan email) dengan ukuran yang besar sehingga sang pemakai tidak dapat membuka emailnya atau kesulitan mengakses emailnya.

Solusi :

- Spam blocker
- Connection limit

4. Non-repudiation

Aspek ini menjaga agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi. Sebagai contoh, seseorang yang mengirimkan email untuk memesan barang tidak dapat menyangkal bahwa dia telah mengirimkan email tersebut. Aspek ini sangat penting dalam hal electronic commerce. Penggunaan digital signature dan teknologi kriptografi secara umum dapat menjaga aspek ini. Akan tetapi hal ini masih harus didukung oleh hukum sehingga status dari digital signature itu jelas legal.

5. Authentication

Aspek ini berhubungan dengan metoda untuk menyatakan bahwa informasi betul-betul asli / orang yang mengakses / memberikan informasi adalah betul-betul orang yang dimaksud. Masalah pertama, membuktikan keaslian dokumen dapat dilakukan dengan teknologi watermarking dan digital signature. Watermarking juga dapat digunakan untuk menjaga "intellectual property", yaitu dengan menandai dokumen / hasil karya dengan "tanda tangan" pembuat. Masalah kedua biasanya berhubungan dengan access control, yaitu berkaitan dengan pembatasan orang yang dapat mengakses informasi. Dalam hal ini pengguna harus menunjukkan bukti bahwa memang dia adalah pengguna yang sah, misalnya dengan menggunakan password, biometric (ciri-ciri khas orang), dan sejenisnya. Penggunaan teknologi smart card saat ini kelihatannya dapat meningkatkan keamanan aspek ini.

6. Access Control

Aspek ini berhubungan dengan cara pengaturan akses kepada informasi. Hal ini biasanyaberhubungan dengan masalah authentication dan juga privacy.

Acces control seringkali dilakukan dengan menggunakan kombinasi user id/password atau dengan menggunakan mekanisme lain.

7. Accountability

Artinya setiap kegiatan user di dalam jaringan akan direkam (logged). User tidak akan mencoba untuk melanggar kebijakan keamanan karena identitas dan segala kegiatannya dapat dikenali sehingga mereka dapat dituntut secara hukum. Accountability mencegah perilaku ilegal.

Masalah pada sistem berbasis accountability:

- Hanya berfungsi bila identitas tidak dapat dipalsukan.
- User kehilangan kepercayaan.

Tanpa access control, user dapat menghancurkan sistem secara keseluruhan. Dengan alasan ini, sistem berbasis accountability biasanya dipadukan dengan sistem berbasis access control.

c. Jenis – jenis Ancaman Keamanan Informasi

Dalam *information security*, ancaman dapat berupa serangan pada *software*, pencurian identitas, sabotase, bahkan penghancuran informasi. Ancaman ini akan berusaha mengambil keuntungan dari kerentanan keamanan.

Selain itu, *software* juga rentan terkena virus, *worms*, *Trojan horses*, dan lain-lain. Banyak yang menganggap ancaman tersebut pada umumnya sama.

Namun, *geeks for geeks* menyebut bahwa kesamaan yang mereka miliki hanya sama-sama ancaman bagi *software*. Di luar itu, mereka memiliki perilaku serta butuh penanganan yang berbeda.

Setelah mengetahui beberapa jenis *InfoSec*, waktunya mengetahui macam ancaman untuk kamu antisipasi

1. Malware

Malware terdiri dari dua kata yaitu *malicious* dan *software*. Pada dasarnya, *malware* berarti *software* berbahaya yang dapat berupa kode program yang mengganggu atau apa pun yang dirancang untuk melakukan aktivitas jahat pada sistem.

Adapun *malware* terbagi menjadi 2 yaitu:

- *infection methods*
- *malware actions*

Malware berdasarkan *infection methods* antara lain adalah virus, worms, trojan, dan bots. Sementara itu, *malware* berdasarkan aksi adalah *adware*, *spyware*, *scareware*, *rootkits*, dan *zombies*.

2. Pencurian kekayaan intelektual

Pencurian kekayaan intelektual berarti pelanggaran terhadap hak kekayaan intelektual suatu pihak seperti hak cipta atau paten.

3. Pencurian identitas

Pencurian identitas artinya ketika seseorang bertindak sebagai orang lain untuk mendapatkan informasi pribadi seseorang atau mengakses informasi penting.

Contohnya, seperti mengakses akun media sosial seseorang dengan menggunakan kredensial milik mereka.

4. Pencurian perangkat dan informasi

Ancaman ini semakin meningkat karena sistem perangkat *mobile* dan informasi yang telah tersebar melalui *mobile* dan *cloud*.

5. Sabotase

Sabotase berarti menghancurkan situs web suatu perusahaan untuk menghilangkan kepercayaan pelanggan pada perusahaan tersebut.

6. Pemerasan informasi

Pemerasan informasi adalah pencurian informasi perusahaan untuk menerima pembayaran sebagai imbalannya.

Contohnya, mengunci file korban sehingga tidak dapat diakses. Umumnya, ini dilakukan untuk memaksa korban membayar sebagai syarat membuka kunci tersebut.

7. Serangan media sosial

Kini, serangan media sosial marak terjadi. Istilah *cyber criminal* bahkan muncul di mana mereka dapat mengidentifikasi sekelompok situs web dan media sosial yang ramai dikunjungi untuk mencuri informasi.

8. Mobile malware

Banyak yang mengatakan bahwa ketika kita terhubung dengan internet, maka bahaya keamanan akan terjadi.

d. Internet

Internet adalah suatu jaringan komunikasi yang memiliki fungsi untuk menghubungkan antara satu media elektronik dengan media elektronik yang lain dengan cepat dan tepat. Jaringan komunikasi tersebut, akan menyampaikan beberapa informasi yang dikirim melalui transmisi sinyal dengan frekuensi yang telah disesuaikan. Untuk standar global dalam penggunaan jaringan internet sendiri menggunakan TCP / IP (*Transmission Control Protocol / Internet Protocol*).

Istilah TCP / IP merupakan bentuk protokol pertukaran paket yang digunakan oleh berbagai pengguna global / dunia. Kemudian, proses untuk menghubungkan antara rangkaian internet disebut dengan "*internetworking*". Menurut salah satu ahli dalam bidang IT, Onno W. Purbo (2005) menjelaskan bahwa pengertian internet adalah suatu media yang digunakan untuk mengefisienkan proses komunikasi menggunakan aplikasi seperti website, email, atau voip.

Sejarah internet

Selanjutnya, masuk pada sejarah internet pertama kali di dunia. Sekitar tahun 1960 – an, Departemen pertahanan Amerika melalui ARPA *(Advanced Research Project Agency*) membuat sistem jaringan yang diberi nama ARPANET. ARPANET sendiri merupakan cikal bakal lahirnya teknologi jaringan. Di Amerika sendiri, teknologi jaringan masih dipakai oleh kalangan terbatas di ruang lingkup kampus sekitar tahun 1980 – an.

Kemudian, protokol standar TCP / IP mulai dipublikasikan pada tahun 1982. Sekitar tahun 1986, didirikanlah NSFNET (*National Science Foundation Network*) yang menggantikan peranan dari ARPANET untuk mewadahi kegiatan riset dan penelitian di Amerika. Dan, pada tahun 1990, ARPANET mulai diturunkan dan dengan layanan yang sama World Wide Web (WWW) mulai diperkenalkan oleh CERN.

Dan akhirnya, pada tahun 1993, mulai dikembangkannya InterNIC untuk mendaftarkan nama domain dari publik. Untuk sejarah internet di Indonesia sendiri, mulai masuk pada tahun 1994 yang diperkenalkan oleh beberapa orang ahli di bidang teknologi informasi saat itu.

Manfaat Internet

1. Bidang Bisnis

   Terkait dengan bidang bisnis sendiri, banyak sekali manfaat internet dan keuntungan yang dapat digunakan, seperti pembuatan website usaha, *e – commerce*, bisnis startup, dan industri kreatif yang lainnya. Faktor penting yang perlu diperhatikan disini adalah ketika anda telah berinteraksi dengan internet, maka secara otomatis

anda akan terhubung dengan seluruh pengguna di seluruh dunia, sehingga jangkauan bisnis menjadi lebih luas.

2. Bidang Pendidikan

   Di dalam bidang pendidikan sendiri, penggunaan internet adalah salah satu faktor penting yang membantu dalam proses belajar dan pembelajaran. Pengguna dapat mengakses dan mendapatkan berbagai informasi terkait dengan modul, artikel, jurnal, pengetahuan umum, dan lain sebagainya. Sehingga, setiap individu dapat menemukan berbagai hal melalui mesin pencari yang terhubung dengan jaringan internet yang stabil dan baik.

3. Bidang Informasi

   Saat ini banyak sekali informasi yang bermunculan melalui berbagai perangkat yang ada. Hal tersebut karena, internet adalah penyedia sumber informasi yang dirasa lebih efektif daripada kita harus menonton atau memakai media elektronik seperti radio, televisi, dan koran untuk mendapatkan informasi, dan berita aktual secara cepat.

   Seusai dengan pengertian internet sendiri, media elektronik di abad ke – 21 banyak yang telah memanfaatkan media internet untuk memberikan informasi secara cepat, dengan jangkauan yang lebih luas. Misalnya saja, perusahaan media cetak selain memberikan berita melalui surat kabar, juga membuka media channel di internet untuk mendapatkan berita tidak hanya dari lingkup dalam negeri saja, tetapi sudah mencakup internasional.

4. Bidang Kesehatan

   Banyak sekali referensi kesehatan, dan jasa untuk layanan pengobatan secara *online*. Hal tersebut merupakan bentuk manfaat internet dalam bidang kesehatan. Anda

cukup dengan mencari berbagai kebutuhan seperti obat, resep, gaya hidup sehat, dan rujukan rumah sakit melalui media internet.

5. Bidang Sosial dan Hiburan

   Bidang terakhir yang banyak dimanfaatkan oleh generasi millennial adalah penggunaan internet untuk mengakses berbagai situs dan media sosial yang ada. Seperti Facebook, Twitter, Instagram, Youtube, dan lain sebagainya. Beberapa platform tersebut menyediakan fitur dan akses yang cukup mudah agar setiap orang dapat terhubung dengan baik meskipun berkomunikasi dengan jarak yang sangat jauh.

e. Wireshark

Wireshark merupakan salah satu tools atau aplikasi *capture* paket data berbasis *open-source* untuk melakukan analisis dan pemecah masalah jaringan. Selain itu juga bisa digunakan untuk pengujian *software* karena mampu membaca konten dari tiap paket trafik data. Analisis kerja jaringan melingkupi berbagai hal, dimulai dari proses menangkap paket-paket data atau informasi yang berlalu lalang dalam jaringan sampai memperoleh informasi penting seperti password email dan lain sebagainya.

Aplikasi ini sebelumnya bernama Ethereal, karena permasalahan merek dagang sehingga diubah namanya menjadi Wireshark. Perkembangan aplikasi ini dilakukan oleh kontribusi relawan ahli jaringan diseluruh dunia dan merupakan kelanjutan dari proyek Gerald Combs pada tahun 1998.

Adapun format file yang didukung oleh Wireshark yaitu .cap dan .erf dan adanya alat deskripsi didalamnya juga mampu menampilkan paket-paket terenskripsi dan sejumlah protokol-protokol yang digunakan pada jaringan internet termasuk WEP dan WPA/WPA2.

Fungsi Wireshark

1. Menganalisis Kinerja Jaringan. Memiliki kemampuan cara kerja dengan menangkap paket-paket data atau informasi dari protokol-protokol yang berbeda dan dari berbagai tipe jaringan yang umum ditemukan dalam trafik jaringan internet. Semua jenis informasi dapat dianalisa dengan menggunakan sniffing yang mana anda akan memperoleh informasi penting seperti kata sandi akun lain.
2. Dapat menganalisa transmisi paket data dalam jaringan, proses koneksi dan transmisi data antar komputer.
3. Dapat mengetahui IP seseorang melalui typingan room.
4. Membaca data secara langsung dari Ethernet, Token-Ring, FDDI, serial (PPP dan SLIP), 802.11 wireless LAN, dan koneksi ATM.
5. Berguna untuk profesional jaringan, administrator jaringan, peneliti, hingga pengembang piranti lunak jaringan, karena wireshark merupakan software untuk melakukan analisa lalu lintas jaringan komputer.
6. Sebagai multi-platform yang dapat berjalan di Windows, Linux, macOS, Solaris, FreeBSD, NetBSD, dan sebagainya.
7. Pengambilan langsung dan analisis offline serta memiliki browser paket tiga-panel standar.

Wireshark memiliki fitur yang lengkap, seperti :

1. Multiplatform, bisa dipakai untuk beberapa basis sistem operasi (Unix, Mac, Windows, serta Linux)
2. Bisa lakukan capture paket data jaringan secara real time
3. Bisa menampilkan informasi protokol jaringan dari paket data secara komplit
4. Paket data bisa disimpan jadi file serta nantinya bisa di buka kembali untuk analisa lebih lanjut
5. Filtering paket data jaringan
6. Pencarian paket data dengan persyaratan spesifik
7. Pewarnaan penampilan paket data untuk memudahkan analisis paket data
8. Menampilkan data statistic
9. Untuk lakukan capture paket data yang keluar maupun masuk pada jaringan, wireshark membutuhkan piranti fisik NIC (Network Interface Card).

f. Wifi

Wifi Secara umum, pengertian Wifi adalah teknologi untuk saling bertukar data menggunakan gelombang radio (secara nirkabel) dengan memanfaatkan berbagai peralatan elektronik. Diperlukan peralatan elektronik seperti misalnya komputer, smartphone, tablet, atau bahkan video game console untuk terhubung dalam jaringan komputer, termasuk internet, melalui Wifi.

Perangkat elektronik tersebut haruslah berada dalam sebuah titik akses (*hotspot*) jaringan nirkabel untuk dapat terhubung dengan Wifi. Dalam suatu jaringan Wifi, biasanya titik

akses memiliki jangkauan hingga 20 meter di dalam ruangan, dan ada pula yang lebih jauh jangkauannya untuk Wifi di luar ruangan.

Wifi sendiri sebetulnya merupakan singkatan dari *Wireless Fidelity*. Pada umumnya, untuk bisa terhubung dengan sebuah perangkat elektronik, Wifi menggunakan frekuensi gelombang radio dalam rentang 2,4GHz s/d 5GHz. Semakin berkembangnya zaman mengubah internet dari yang sebelumnya hanya merupakan kebutuhan tersier, kini seakan-akan sudah menjadi kebutuhan primer.

Fungsi Wifi

Setelah memahami pengertian Wifi di atas, tentu kita sudah bisa memahami bahwa salah satu fungsi Wifi adalah untuk menghubungkan perangkat ke dalam jaringan lokal maupun jaringan internet. Namun apakah hanya sebatas itu saja fungsi Wifi? Ternyata, masih ada lagi fungsi Wifi yang mungkin belum Anda sadari, seperti beberapa fungsi di bawah ini misalnya :

1. Menghubungkan perangkat ke dalam jaringan

   Berbeda dengan jaringan kabel LAN yang terbatas penggunanya, Wifi bisa digunakan di banyak komputer tanpa menambah jumlah kabel. Dengan begitu, Wifi memudahkan banyak pengguna untuk sekaligus terhubung ke dalam jaringan.

2. Berbagi data antar perangkat

   Misalkan Anda mempunyai dua buah perangkat elektronik, lalu ingin memindahkan data di salah satunya ke perangkat lainnya. Wifi dapat dimanfaatkan untuk hal ini,

sehingga kabel data tak lagi dibutuhkan dan menyebabkan pekerjaan lebih praktis dan efisien.

3. Modem dari smartphone

   Memang dengan adanya Wifi, sebuah smartphone dapat terhubung dengan internet sehingga pengguna tak perlu lagi menggunakan paket data berbayarnya. Namun tak hanya itu, jika smartphone Anda mendukung perangkat wireless, maka Anda bisa menjadikan smartphone tersebut sebagai modem.

   Hal ini sangat berguna terutama jika Anda bepergian ke tempat yang tidak tersedia Wifi. Jika paket data Anda cukup banyak, maka ketika ingin mengakses internet melalui laptop misalnya, Anda dapat memfungsikan smartphone sebagai modem yang menggunakan sinyal Wifi untuk terhubung ke laptop.

4. Kecepatan internet lebih pesat

   Hal ini tentu sudah bisa dipahami oleh para pengguna smartphone. Berbeda dengan saat mengakses internet melalui jaringan seluler yang terkadang cepat terkadang lambat tergantung keberadaan sinyal, biasanya kecepatan akses internet dengan menggunakan Wifi lebih terjamin kecepatannya. Salah satu indikasinya adalah Anda bisa melakukan streaming video tanpa putus-putus, pengunduhan dokumen yang lebih cepat, akses yang tidak membutuhkan loading.

g. Protokol Jaringan

Protokol adalah sistem peraturan yang memungkinkan terjadinya hubungan, komunikasi, dan perpindahan data antara dua komputer atau lebih. Aturan ini harus dipenuhi oleh pengirim dan penerima agar komunikasi dapat berlangsung dengan baik.

Sederhananya, protokol adalah media yang digunakan untuk menghubungkan pengirim dan penerima. Protokol dapat diterapkan pada perangkat keras dan perangkat lunak. Jadi hampir semua komunikasi yang terjadi pada jaringan komputer pasti melibatkan protokol.

Sebagai contoh, seperti orang yang mengirimkan email. Email dalam komputer bisa disebut dengan sebuah data. Sehingga email yang dikirimkan pada seseorang dari komputer satu ke komputer lain sebenarnya adalah pengiriman data.

Setiap orang mengirimkan email, pasti email akan melewati beberapa protokol. Semua protokol harus dilalui agar email bisa keluar dan diterima komputer lain pada jaringan yang sama atau berbeda.

Fungsi protocol jaringan

Protokol memegang peran yang cukup vital dalam perpindahan data di internet. Secara umum fungsi protokol adalah untuk menghubungkan antara pengirim dan penerima agar bisa berkomunikasi. Secara lebih khusus, berikut ini adalah fungsi-fungsi protokol:

1. Addressing

   Header IP paket mengandung alamat yang memberikan identifikasi ke komputer pengirim dan penerima. Router menggunakan informasi ini untuk menuntun setiap paket melewati network komunikasi dan menghubungkan antara komputer pengirim dan penerima.

2. Reassembly

   Kegunana internet protokol adalah memastikan pesan dipecah menjadi paket. Hal ini dikarenakan sebagian besar pesan terlalu besar untuk dimasukan ke dalam satu paket,

dan karena paket tidak dikirimkan dalam urutan yang benar. Paket harus tersusun ulang saat tiba di penerima.

3. Timeouts

   Setiap IP paket mengandung self-destructive counter yang membatasi umur dari paket. Jika paket sudah kadaluarsa, paket dihancurkan sehingga jaringan internet tidak mengalami overloaded dengan paket yang rusak.

4. Options

   IP terdapat fitur tambahan yang mengizinkan komputer pengirim untuk memutuskan paket bagian mana yang didapatkan komputer penerima. Untuk menemukan bagian yang diambil maka perlu ditambahkan keamanan pada paket.

h. Web Server

Web server adalah perangkat lunak yang berfungsi sebagai penerima permintaan yang dikirimkan melalui browser kemudian memberikan tanggapan permintaan dalam bentuk halaman situs web atau lebih umumnya dalam dokumen HTML. Namun, web server dapat mempunyai dua pengertian berbeda, yaitu sebagai bagian dari perangkat keras (hardware) maupun sebagai bagian dari perangkat lunak (software).

Jika merujuk pada hardware, web server digunakan untuk menyimpan semua data seperti HTML dokumen, gambar, file CSS stylesheets, dan file JavaScript. Sedangkan pada sisi software, fungsi web server adalah sebagai pusat kontrol untuk memproses permintaan yang diterima dari browser web.

Jadi sebenarnya semua yang berhubungan dengan website biasanya juga berhubungan dengan web server, karena tugas web server adalah mengatur semua komunikasi yang terjadi antara browser dengan server untuk memproses sebuah website.

Saat ini ada beberapa pilihan web server saat ini tersedia, nanti akan kami coba bahas satu persatu mengenai kelebihan masing-masing web server. Sebelumnya, mari kita coba bahas mengenai bagian lain dari web server.

Pada tahun 1990 web server adalahproyek yang diusulkannya pada atasannya di CERN (Organisasi Riset Nuklir Eropa) bernama CERN httpd yang diusulkan oleh Sir Tim Berners-Lee. Web server ini berjalan pada server NeXT. NeXT merupakan perusahaan yang didirikan oleh Steve Jobs setelah keluar dari Apple.

Pada tahun yang sama ditemukan pula browser pertama kali yang dinamakan WorldWideWeb.

Jadi, selain berfungsi sebagai komunikasi penghubung dengan situs web dan memproses HTTP request yang dikirimkan oleh browser, secara umum beberapa fungsi web server adalah sebagai berikut:

1. Memastikan semua modul yang dibutuhkan tersedia dan siap digunakan
2. Membersihkan penyimpanan, cache, dan module yang tidak terpakai
3. Melakukan pemeriksaan keamanan terhadap HTTP request yang dikirimkan browser