UJIAN AKHIR SEMESTER KEAMANAN INFORMASI

Nama : Adhe Pandu Dwi Prayogha
Kelas : TI – A
Nim : 1310651046

SOAL NO 1.

Pokok Permasalahan
Domain 2: Telecommunications and Network Security

Bagian pertama kami adalah arsitektur jaringan dan desain. Kita akan membahas bagaimana jaringan harus dirancang dan kontrol mereka mungkin berisi, dengan fokus pada penggelaran pertahanan-mendalam strategi dan menimbang biaya dan kompleksitas dari kontrol jaringan versus manfaat disediakan.

Konsep jaringan dasar

Sebelum kita dapat membahas Telekomunikasi spesifik dan konsep Keamanan Jaringan, kita perlu memahami konsep dasar di belakang mereka. Istilah seperti broadband sering digunakan secara informal: ujian memerlukan pemahaman yang tepat dari informasi terminologi keamanan.

Simplex, half-duplex, dan komunikasi full-duplex

Komunikasi simpleks satu arah, contoh walki talkie

LAN, WAN, MAN, dan PANS

Sebuah LAN atau Local Area Network. Jaringan yang jangkauanya relatif kecil, hanya antar gedung saja.

Sebuah MAN atau Metropolitan Area Network,
yang biasanya jangkauanya terbatas pada sebuah kampus, perkantoran dll.

Sebuah WAN atau Wide Area Network, biasanya meliputi kota, negara.

PANS atau Personal Area Networks, dengan jarak berkisar 100 m atau kurang. Teknologi nirkabel daya rendah seperti Bluetooth digunakan untuk membuat PANS.

OSI MODEL

OSI (Open Sistem Interkoneksi) Model Referensi adalah jaringan Layered Model. Model ini bersifat abstrak

Layer 1: Physical

Layer 1 model OSI. Lapisan 1 menggambarkan unit data tersebut sebagai bit diwakili oleh energi seperti cahaya, listrik, atau gelombang radio dan media yang digunakan : kabel tembaga atau fiber optik.

Layer 2: Data Link

Data Link Layer bertugas menangani akses ke layer Physical serta Local Area Network komunikasi. Kartu Ethernet dan MAC (Media Access Control) address berada di Layer 2, seperti switch dan jembatan.

Layer 3: Jaringan/Network

Layer Jaringan bertugas memindahkan data dari sistem pada satu LAN ke sistem yang lain. Alamat IP dan router ada pada Layer 3. Layer 3 protokol termasuk IPv4 dan IPv6.

Layer 4: Transport
Transport Layer bertugas menangani paket sequencing, pengontrol aliran, dan deteksi kesalahan. TCP dan UDP adalah Layer 4 protokol. membuat sejumlah fitur yang tersedia, seperti pengiriman ulang atau resequencing paket.
Layer 5: Session
Session Layer mengelola session, yang menyediakan perawatan pada koneksi.
Mount berbagi file lewat jaringan memerlukan sejumlah sesi maintance, seperti sebagai Remote Procedure Calls (RPC): ini ada di Session Layer.
Layer 6: Presentation
Presentation Layer menyajikan data ke aplikasi (dan pengguna) dalam cara pemahaan
Konsep Presentation Layer meliputi konversi data,seperti ASCII, picture berformat seperti GIF, dan TIFF.
TCP / IP model
Model TCP / IP (Transmission Control Protocol / Internet Protocol) adalah populer model jaringan yang dibuat oleh AS Defense Advanced Research Projects Agency pada 1970-an. TCP / IP adalah nama informal (dinamai dua protokol pertama dibuat); nama resmi adalah Internet Protocol Suite. Model TCP / IP lebih sederhana dari model OSI, seperti yang ditunjukkan pada Tabel 2.2.
Sementara TCP dan IP menerima tagihan atas, TCP / IP sebenarnya merupakan suite protokol termasuk UDP (User Datagram Protocol) dan ICMP (Internet Control Message Protocol), di antara banyak lainnya.

TCP / IP model

Model TCP / IP (Transmission Control Protocol / Internet Protocol) adalah medel jaringan terpopuler yang dibuat oleh AS Defense Advanced Research Projects Agency
pada 1970-an. TCP / IP adalah nama informal (dinamai dua protokol pertama
dibuat.

Network Acess Layer
Jaringan Access Layer dari model TCP / IP menggabungkan Layer 1 (Physical) dan Layer 2 Data Link dari model OSI. Ini menggambarkan 1 masalah seperti energi, bit, dan media yang digunakan untuk membawa media seperti tembaga, serat, nirkabel, dll. Ini tentunya juga menjelaskan tentang Layer 2, isu-isu yang mengkonversi bit menjadi unit-unit protokol seperti Ethernet frame, MAC (Media Access Control) alamat, dan Network Interface Cards (NIC).
Internet layer
Layer Internet dari model TCP / IP sejalan dengan Layer 3 Network, Lapisan model OSI. Pada inilah alamat IP dan routing dapat aktif. Ketika data ditransmisikan dari node pada satu LAN ke node pada LAN yang berbeda, Layer Internet yang digunakan.

Host-to-Host Transport Layer
Host-to-Host Transport Layer bertugas menghubungkan Internet
Lapisan ke Application Layer. di mana aplikasi yang ditujukan pada jaringan, melalui port
Application Layer
TCP / IP Application Layer menggabungkan Layer 5 sampai 7 yaitu Session, Presentation, dan Aplikasi dari OSI Model. Sebagian besar dari protokol menggunakan arsitektur bersifat client-server,
di mana klien (seperti ssh) terhubung ke server mendengarkan (disebut daemon pada Sistem UNIX).

MAC address
Sebuah Media Access Control (MAC) adalah alamat hardware yang unik dari Ethernet kartu jaringan Interface (NIC),. MAC alamat dapat diubah dalam perangkat lunak.
IPv4
IPv4 adalah Internet Protocol versi 4,. Ini adalah protocol Dasar dari internet, dirancang pada tahun 1970 untuk mendukung packet-switched jaringan bagi AS Defense Advanced Research Projects Agency (DARPA). IPv4 digunakan untuk ARPAnet, yang kemudian menjadi Internet.
IP adalah protokol sederhana, dirancang untuk membawa data melalui jaringan.
IPv6
IPv6 adalah Terusan IPv4, memiliki fitur menampilkan ruang alamat yang jauh lebih besar (alamat 128-bit dibandingkan dengan IPv4 yang 32 bit), routing sederhana , dan alamat sederhana. kurangnya alamat IPv4 adalah faktor utama yang menyebabkan terciptanya IPv6.
TCP
TCP adalah Transmission Control Protocol, Layer 4 protokol yang handal. TCP menggunakan Three way handshake untuk membuat koneksi yang dapat diandalkan di seluruh jaringan.

Application-Layer TCP/IP protocols and concepts

Telnet
Telnet menyediakan emulasi terminal melalui jaringan. Server Telnet mendengarkan pada port TCP 23.
FTP
FTP adalah File Transfer Protocol, digunakan untuk mentransfer file ke dan dari server.
SSH
SSH dirancang sebagai pengganti yang aman untuk Telnet, FTP, dan UNIX "R" perintah (rlogin, rshell, dll). Ini menyediakan kerahasiaan, integritas, dan otentikasi aman, antara fitur-fitur lainnya.
SMTP, POP, dan IMAP
SMTP adalah Simple Mail Transfer Protocol, digunakan untuk mentransfer e-mail antara server.
DNS
DNS adalah Domain Name System, database hirarki global yang terdistribusi yang menerjemahkan nama ke alamat IP dan sebaliknya.
HTTP dan HTTPS
HTTP adalah Hypertext Transfer Protocol, yang digunakan untuk mentransfer terenkripsi Data berbasis web.

LAN technologies and protocols

Local Area Network konsep Berfokus pada Layer 1-3 teknologi seperti jaringan jenis kabel, topologi jaringan fisik dan logis, Ethernet, FDDI, dan lain-lain.
Ethernet
Ethernet beroperasi pada Layer 2 dan merupakan dominan lokal teknologi Jaringan di Area yang mentransmisikan data jaringan melalui frame.

Teknologi WAN dan protokol

ISP dan lainnya "jarak jauh" penyedia jaringan, yang jaringan span dari kota ke negara, sering menggunakan teknologi Wide Area Network.
T1s, T3s, E1s, dan E3s
Ada sejumlah standar sirkuit internasional: yang paling umum adalah T-operator (Amerika Serikat) dan E-operator (Eropa).

FAST FACTS

Here is a summary of common circuits:
•AT1 is a dedicated 1.544-megabit circuit that carries 2464-bit DS0(Digital Signal 0) channels.
•AT3 is 28 bundled T1s, forming a 44.736-megabit circuit.
•AnE1 is a dedicated 2.048-megabit circuit that carries 30 channels.
•AnE3 is 16 bundled E1s, forming a 34.368-megabit circuit.

Teknologi WAN dan protokol

ISP dan lainnya "jarak jauh" penyedia jaringan, yang jaringan span dari kota ke negara, sering menggunakan teknologi Wide Area Network.

T1s, T3s, E1s, dan E3s

Ada sejumlah standar sirkuit internasional: yang paling umum adalah T-operator (Amerika Serikat) dan E-operator (Eropa).

FAKTA CEPAT

Berikut adalah ringkasan dari sirkuit umum:

- AT1 adalah sirkuit 1,544-megabit khusus yang membawa 2.464-bit DS0 (Digital Signal 0) saluran.
- AT3 adalah 28 paket T1s, membentuk sirkuit 44,736-megabit.
- AnE1 adalah sirkuit 2,048-megabit khusus yang membawa 30 saluran.
- AnE3 adalah 16 E1s dibundel, membentuk sirkuit 34,368-megabit.

Frame Relay

Frame Relay adalah protokol WAN Layer 2 packet-switched yang menyediakan tidak ada kesalahan pemulihan dan berfokus pada kecepatan.

Frame Relay

Frame Relay adalah protokol WAN Layer 2 packet-switched yang menyediakan tidak ada kesalahan pemulihan dan berfokus pada kecepatan.

NETWORK DEVICES AND PROTOCOLS

Repeater dan hub

Repeater dan hub adalah Layer 1 perangkat. Sebuah repeater yang menerima bit pada satu port dan "Mengulangi" port yang lainnya.

Bridges

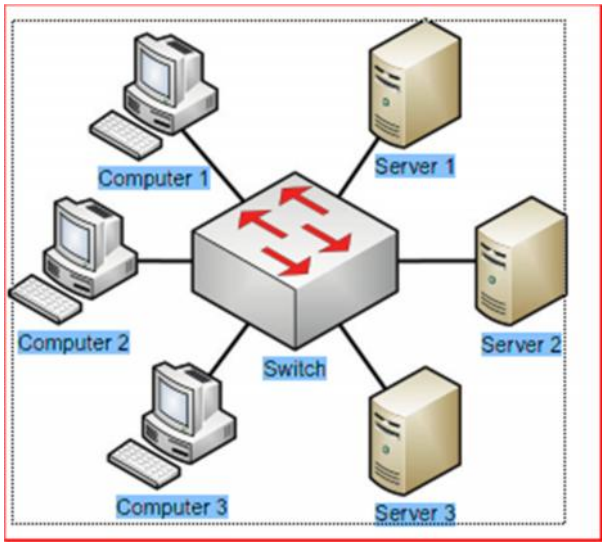
Bridge dan switch adalah Layer 2 perangkat. Sebuah jembatan memiliki dua port dan menghubungkan jaringan segmen bersama-sama.

Provider

isolasi lalu lintas dan membuat keputusan forwarding dengan mempelajari MAC alamat node terhubung. Sebuah jembatan memiliki dua domain tabrakan.

Switch

Switch adalah sebuah jembatan dengan lebih dari dua port. Juga, itu adalah praktek terbaik untuk hanya menghubungkan satu perangkat per port switch.



router
Router adalah Layer 3 perangkat yang rute lalu lintasnya dari satu LAN ke LAN yang lain. IP berbasis router membuat keputusan routing berbasis pada sumber dan tujuan alamat IP yang dituju
firewall
Firewall menyaring lalu lintas antara jaringan. TCP / IP packet filter dan firewall stateful membuat keputusan berdasarkan Layers 3 dan 4 (alamat IP dan port). Firewall Proxy bisa juga membuat keputusan berdasarkan Layers 5-7. Firewall multihomed: mereka memiliki beberapa NIC terhubung ke beberapa jaringan yang berbeda.
Modem
Modem adalah modulator / demodulator. Dibutuhkan data biner dan memodulasi itu menjadi suara analog yang dapat dilakukan pada jaringan telepon dirancang untuk membawa suara manusia
Intrusion Detection Systems dan Intrusion Prevention System
Sebuah Intrusion Detection System (IDS) adalah perangkat detektif yang dirancang untuk mendeteksi berbahaya
(Termasuk melanggar kebijakan-) tindakan. Sebuah Intrusion Prevention System (IPS) adalah perangkat preventif dirancang untuk mencegah tindakan jahat.
Endpoint security
Karena titik akhir adalah target serangan, kemampuan pencegahan dan detektif endpoint sendiri memberikan lapisan pertahanan luar keamanan jaringan-sentris perangkat.
Banyak produk titik dapat dianggap sebagai bagian dari keseluruhan Suite keamanan endpoint.
Anti Virus
Yang paling umum digunakan produk keamanan endpoint adalah perangkat lunak antivirus. Anti Virus adalah satu lapisan (banyak) pertahanan keamanan endpoint secara mendalam. Meskipun antivirus vendor sering menggunakan metode heuristik atau statistik untuk deteksi malware, dominan berarti mendeteksi malware masih signature berbasis.

SECURE COMMUNICATIONS
Melindungi data dalam gerak adalah salah satu tantangan yang paling kompleks yang kita hadapi.
Internet
menyediakan komunikasi-dengan global yang murah sedikit atau tidak ada built-in kerahasiaan, integritas, atau ketersediaan.
PAP dan CHAP
PAP (Password Authentication Protocol) adalah protokol otentikasi sangat lemah. misalkan Saya mengirimkan username dan password dalam teks-jelas. Penyerang yang mampu mendeteksi proses otentikasi dapat meluncurkan serangan replay sederhana, dengan memutar username dan password, menggunakan mereka untuk login. PAP tidak aman dan tidak boleh digunakan.
802.1X dan EAP
802.1X adalah "Jaringan Port-Based Access Control" dan termasuk EAP (Extensible Authentication Protocol). EAP adalah kerangka kerja otentikasi yang menggambarkan banyak protokol otentikasi yang spesifik. EAP dirancang untuk menyediakan otentikasi pada Layer ke2 (itu adalah "port berdasarkan," seperti port pada switch), sebelum simpul menerima alamat IP.
VPN
Virtual Private Networks (VPN) data yang aman dikirim melalui jaringan yang tidak aman contohnya seperti Internet. Tujuannya adalah untuk memberikan privasi yang diberikan oleh sirkuit seperti T1,
Remote meeting technology
Teknologi pertemuan jarak jauh adalah teknologi baru yang memungkinkan pengguna untuk melakukan secara online
pertemuan melalui internet, termasuk fungsi desktop sharing.

SOAL NO 2.

Aplikasi Steganografi
Quick Stego

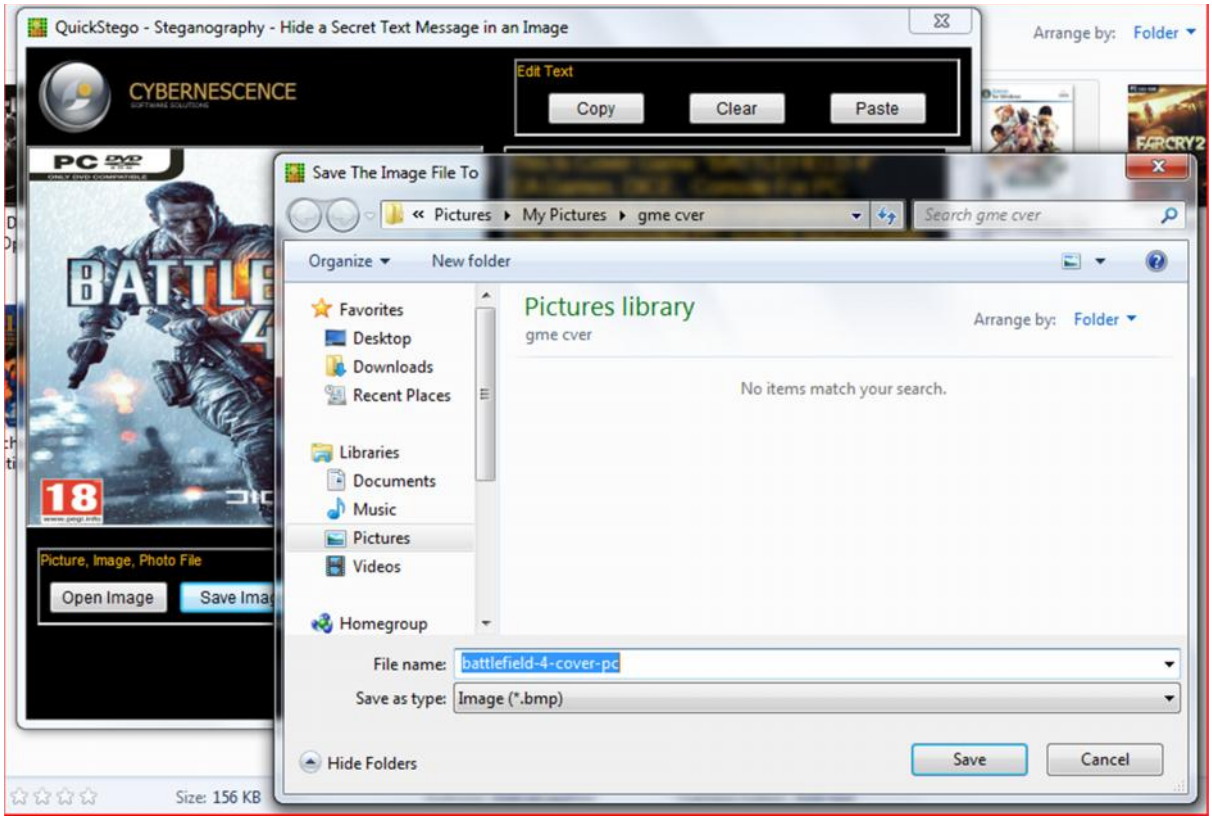
Ini adalah Tampilan dari Software Quick Stego.

Selanjutnya Pilih Gambar dengan mengklik Button “Open Image” pada pojok kiri bawah,
Pilih Gambar Pada file directory anda.,

Setelah Memilih Gambar, Misalkan Contoh saya memilih Gambar Cover Game “BATTLEFIELD 4”.,

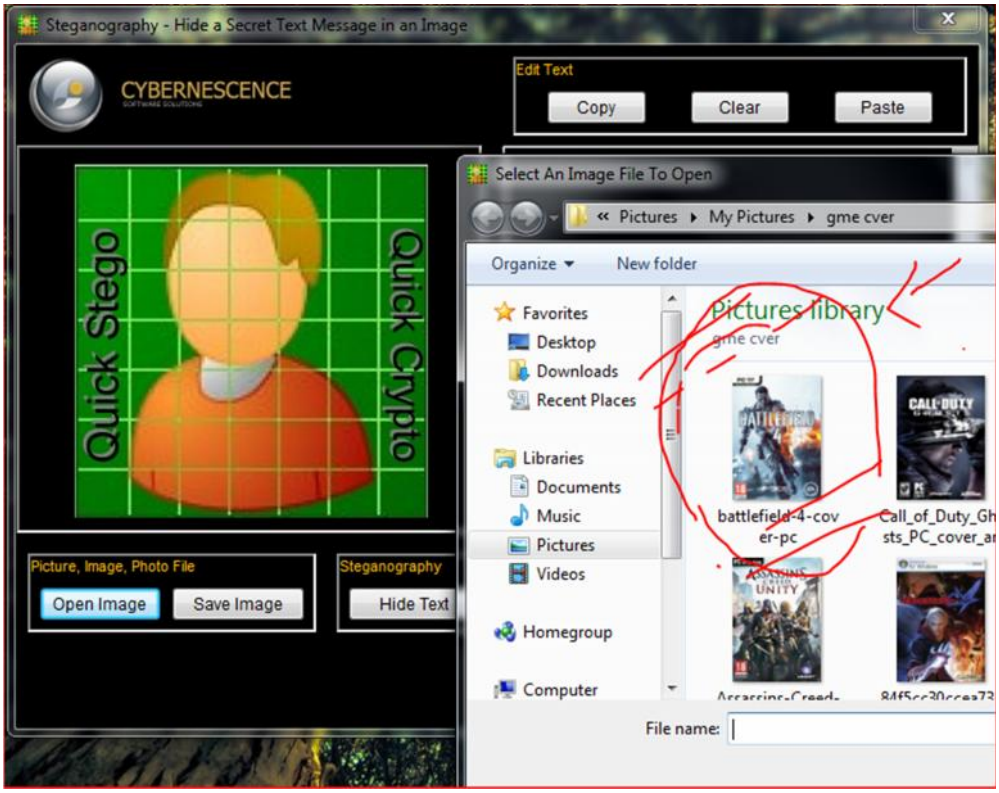
Selanjutnya Ketikan Text apa saja, atau Hal yang berkaitan dengan gambar yang anda pilih pada kolom di sebelah kanan cover gambar.

Setelah itu Klik “Button Hide Text” pada kolom Steganography. Maka anda akan menerima Message/Pesan “The Text Message is Now Hidden in Image”. Setelah itu Klik Save.



Setelah Gambar Di Save Secara Otomatis Text yang ada pada gambar tersebut menjadi Tersembunyi/Hidden pada gambar tersebut. Dan Exit pada software tersebut.

Dan selanjutnya jika anda ingin membuka/melihat text yang tersembunyi, dapat membuka kembali Gambar yang telah anda save. Open Software Quick Stego, Open Image, pilih gambar yang anda save.



Setelah Gambar yang ada save Dibuka, Otomatis Text Tersembunyi Tersebut akan Terlihat Lagi seperti Gambar Diatas.