Government Computer Security Incident Response Team

BADAN PENGKAJIAN DAN PENERAPAN TEKNOLOGI

PANDUAN PENANGANAN INSIDEN
KEAMANAN JARINGAN

Diadopsi dari : SOP Incident Handling Networking
Kementrian Komunikasi dan Informastika Republik Indonesia

BUKU PETUNJUK PELAKSANAAN

BPPT CSIRT
2014

DAFTAR ISI

BAGIAN 1 : PENDAHULUAN

Penanganan Insiden Keamanan Jaringan adalah bagian dalam menangani keamanan informasi. Sebab dari keadaan jaringan yang ada dan diaplikasikan dalam suatu organisasi akan mempengaruhi keamanan informasi yang ada padanya.

1.1 TUJUAN

Tujuan dari prosedur ini adalah untuk memastikan manajemen yang efektif dan konsisten dari penanganan insiden keamanan pada jaringan komputer. Tujuan Informasi ini adalah untuk mengenalkan kepada personel keamanan TI terhadap serangan pada jaringan (misal Distributed denial-of-service), modus operandi, dan langkah-langkah yang direkomendasikan untuk membantu upaya perbaikan, persiapan, identifikasi, penahanan, pemulihan dan keberlangsungan yang diperlukan untuk membatasi risiko yang diakibatkan oleh terjadinya insiden. Dokumen ini dapat digunakan oleh administrator sistem, tim insiden respon insiden keamanan komputer, pusat operasi keamanan TI dan kelompok teknologi terkait lainnya.

1.2 RUANG LINGKUP

Informasi ini ditujukan untuk profesional TI dan manajer dalam organisasi di BPPT. Para penerima produk ini lebih lanjut dapat mendistribusikannya kepada para pemangku kepentingan teknis dalam organisasi mereka. Insiden keamanan pada jaringan bisa bermacam-macam, prosedur penanganan disini difokuskan pada penanganan insiden untuk,

1. Denial of Service
 Single or distributed (DoS or DDoS)

 Inbound or outbound
2. Reconnaissance activity
 Port scanning
 Network vulnerability scanning
 Unauthorized network monitoring
3. Unauthorized access
 Unauthorized access to network
 Inappropriate Usage

Definisi

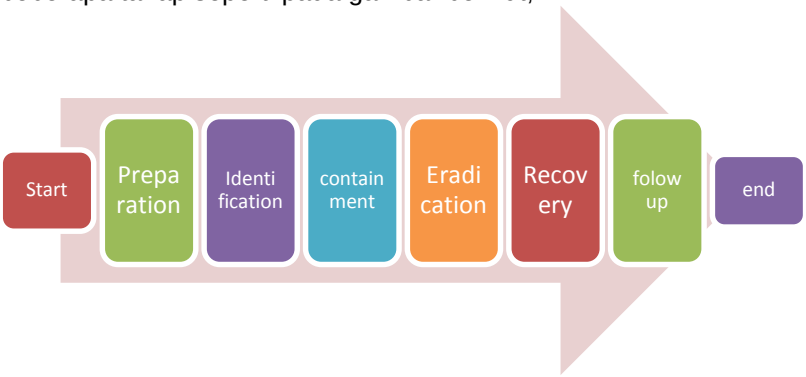
Denial of service (DoS) umumnya merupakan tindakan serangan berbahaya pada jaringan yang ditujukan untuk mengganggu ketersediaan sumber daya komputasi dari pengguna yang sah. Serangan DDoS baru-baru ini mendapatkan popularitas karena ketersediaan dari jasa penyewaan DoS dari operator botnet, serta ketersediaan berbagai alat hacking gratis dan mudah digunakan. Sebuah serangan DDoS terjadi ketika beberapa sistem secara bersamaan membanjiri sumber daya jaringan komputer, membuat mereka tidak dapat diakses. Berbeda dengan serangan DoS, sebuah serangan DDoS, berasal dari berbagai sumber, bisa ratusan atau bahkan ribuan. Akibatnya, tindakan mitigasi terhadap serangan DDoS lebih sulit. Serangan DDoS sering menggunakan protokol seperti UDP dan ICMP, tetapi protocol stateful juga dapat digunakan ketika koneksi tidak sepenuhnya mapan seperti selama serangan membanjirnya TCP SYN. Kedua teknik memudahkan penyerang untuk menggunakan alamat IP palsu dan sulit untuk menentukan sumber serangan.

BAGIAN 2 :

PROSEDUR PENANGANAN INSIDEN KEAMANAN JARINGAN

Secara umum tahap-tahap dalam menangani suatu insiden dapat digambarkan sebagai berikut :

Penangan terhadap insiden keamanan Jaringan dapat dilakukan dalam beberapa tahap seperti pada gambar berikut,



Gambar 1 : Tahap-tahap penanganan insiden

2.1. Tahap Persiapan (Preparation)

Persiapan adalah langkah yang paling penting dalam menangani serangan yang terjadi pada jaringan komputer. Prosedur dan pedoman yang jelas dan lengkap harus disiapkan secara matang sebelum serangan terjadi. Setiap organisasi dapat menjadi korban serangan pada jaringan, baik secara langsung maupun tidak langsung. Memiliki rencana yang solid akan membantu mengurangi risiko dan mengurangi dampak

buruk dari serangan yang terjadi. Persiapan yang dilakukan meliputi,

Persiapan Personal

Meskipun memiliki kendali proses dan teknis yang kuat, keamanan dapat dikompromikan dengan memanfaatkan personil dan membuat mereka melakukan tindakan yang sebaliknya tidak diizinkan. Tim penanganan insiden yang terampil dan adanya matrik eskalasi merupakan komponen kunci dari startegi penanganan dan penahanan yang efektif. Sebuah tim penanganan insiden yang baik adalah sumber daya sangat berharga ketika dibutuhkan untuk menangani situasi yang mungkin timbul karena adanya malware, dengan cara yang efisien dan efektif. Sebagaimana orang adalah sumber daya organisasi utama yang akhirnya dirugikan oleh infeksi malware, kesadaran akan keamanan merupakan salah satu dari isu-isu yang perlu terus menerus dipantau dan ditingkatkan untuk perlindungan yang tepat dari berbagai serangan. Menetapkan peran dan tanggung jawab, identifikasi siapa yang berperan dalam menangani serangan pada jaringan dan memastikan mereka menyadari tanggung jawabnya. Ini harus mencakup personel dari semua fungsi kritis bisnis, operasional TI, tim jaringan dan keamanan TI, penasihat hukum, dan staf hubungan media. Memastikan daftar kontak tim up-to-date, baik kontak utama maupun alternatifnya. Sebagaimana kemungkinan tidak tersedianya jaringan, termasuk perangkat mobile, maka harus membuat mekanisme cara berkomunikasi melalui media alternatif lain. Menetapkan prosedur dengan Internet Service Provider (ISP) untuk menentukan bagaimana mereka dapat membantu organisasi selama terjadinya serangan pada jaringan. Mengetahui tentang Service Level Agreement (SLA) yang ada dan biaya- biaya apa yang mungkin timbul. Menetapkan informasi kontak selama 24jam 7 hari untuk ISP dan metode alternative untuk komunikasi

Persiapan Teknologi/tool

Persiapan teknologi adalah kegiatan untuk menyiapkan semua alat/teknologi yang diperlukan dalam proses penanganan insiden keamanan pada jaringan, alat-alat tersebut antara lain,

a. Virus Removal Tools:

Komponen lain yang harus disediakan dalam penanganan insiden pada jaringan adalah tool dari berbagai vendor antivirus untuk menghapus malware. Tool penghapus virus bisa lebih efektif, efisien, dan mudah untuk bekerja daripada mesin antivirus. Namun, tool tersebut terbatas hanya bekerja sebagian besar satu keluarga malware. McAfee Stringer adalah alat removal untuk suatu kelompok malware.

b. Wireshark

Wireshark adalah sebuah tools open source yang berfungsi sebagai network packet analyzer. Sebuah network packet analyzer akan berusaha meng-capture packet data dan menampilkan sedetail mungkin jika memungkinkan. Wireshark merupakan salah satu dari sekian banyak tool Network Analyzer yang banyak digunakan oleh Network administrator untuk menganalisa kinerja jaringannya terrmasuk protokol didalamnya. Wireshark banyak disukai karena interfacenya yang menggunakan Graphical User Interface (GUI) atau tampilan grafis. Wireshark mampu menangkap paket-paket data atau informasi yang berseliweran dalam jaringan. Semua jenis paket informasi dalam berbagai format protokol pun akan dengan mudah ditangkap dan dianalisa. Karenanya tak jarang tool ini juga dapat dipakai untuk sniffing (memperoleh informasi penting spt password email atau account lain) dengan menangkap paket-paket yang berseliweran di dalam jaringan dan menganalisanya.

c. Metasploit

Metasploit merupakan sofware security yang sering digunakan untuk menguji coba ketahanan suatu sistem dengan cara mengeksploitasi kelemahan software suatu sistem. Metasploit biasanya digunakan untuk menyerang application layer dengan 0 day attack yang merupakan metode penyerangan pada software yang belum di patch. Metasploit biasa dikaitkan dengan istilah remote exploitation, maksudnya penyerang

berada pada jarak jangkauan yang jauh dapat mengendalikan komputer korban. Metasploit menyerang dengan cara mengirimkan exploit pada komputer korban. Exploit ini berisi payload yang sudah ditentukan oleh penyerang. Exploit adalah software yang berfungsi untuk memanfaatkan kelemahan pada software korban(misal web browser), setelah berhasil mengeksploitasinya exploit tersebut memasukkan payload ke dalam memori korban. **Payload merupakan sebuah executable milik penyerang yang akan di run pada komputer korban dengan tujuan dapat mengendalikan komputer tersebut secara remote atau memasang backdoor, trojan, virus, worm, dan lain-lain.** Terlepas dari penggunaan metasploit yang disalah gunakan untuk kejahatan, software ini juga membantu System Security untuk memperkuat pertahanan jaringannya dari ulah penyerang dari luar.

Persiapan Dokumen yang dibutuhkan

a. Membuat daftar dari alamat IP yang diprioritaskan untuk diperbolehkan melewati jaringan selama penanganan insiden.

b. Menyiapkan dokumen topologi jaringan, termasuk semua alamat IP yang paling up to date.

c. Meninjau Disaster Recovery Plan (DRP) dan memastikan manajemen senior dan tim hukum memahami pentingnya penanganan dari serangan pada jaringan, termasuk peran mereka.

Persiapan Komponen Keamanan Network

Komponen keamanan jaringan adalah komponen-komponen yang selama ini digunakan oleh organisasi untuk menjaga keamanan pada jaringan komputer dari organisasi tersebut, komponen-komponen itu antara lain,

Anti Malware

Anti malware merupakan sistem perangkat lunak yang berfungsi untuk

menangkal program-program jahat yang akan memasuki/menyusup ke dalam jaringan komputer.

Firewall
Firewall adalah sebuah sistem atau perangkat yang mengizinkan lalu lintas jaringan yang dianggap aman untuk melaluinya dan mencegah lalu lintas jaringan yang tidak aman. Firewall umumnya juga digunakan untuk mengontrol akses terhadap siapa saja yang memiliki akses terhadap jaringan pribadi dari pihak luar.

Fungsi Firewall :

- Mengontrol dan mengawasi paket data yang mengalir di jaringan Firewall harus dapat mengatur, memfilter dan mengontrol lalu lintas data yang diizinkan untuk mengakses jaringan privat yang dilindungi firewall. Firewall harus dapat melakukan pemeriksaan terhadap paket data yang akan melewati jaringan privat. Beberapa kriteria yang dilakukan firewall apakah memperbolehkan paket data lewat atau tidak, antara lain :
  - ✓ Alamat IP dari komputer sumber
  - ✓ Port TCP/UDP sumber dari sumber
  - ✓ Alamat IP dari komputer tujuan
  - ✓ Port TCP/UDP tujuan data pada komputer tujuan
  - ✓ Informasi dari header yang disimpan dalam paket data
  - ✓ Melakukan autentifikasi terhadap akses

- Applikasi proxy Firewall mampu memeriksa lebih dari sekedar header dari paket data, kemampuan ini menuntut firewall untuk mampu mendeteksi protokol aplikasi tertentu yang spesifikasi

- Mencatat setiap transaksi kejadian yang terjadi di firewall. Ini Memungkinkan membantu sebagai pendeteksian dini akan penjebolan jaringan IDS/IPS Intrusion detection system (IDS) adalah perangkat yang memiliki kemampuan dalam melakukan pendeteksian terhadap serangan dan ancaman yang terjadi pada

sebuah jaringan computer baik secara lokal maupun yang sudah terkoneksi dengan internet. IDS merupakan salah satu intrusion detection system (IDS) yang mendeteksi penyusupan jaringan komputer. IDS hanya melakukan pendeteksian terhadap suatu host resource pada log yang dihasilkan dengan memonitor system file.

VPN

VPN adalah singkatan Virtual Private Network, yaitu sebuah koneksi yang bersifat private melalui jaringan publik atau internet, virtual network berarti jaringan yang terjadi hanya bersifat virtual. Private berarti jaringan yang terbentuk bersifat private dimana tidak semua orang bisa mengaksesnya. Data yang dikirimkan terenkripsi, sehingga kerahasiaan data akan terjamin meskipun melalui jaringan publik. Jika menggunakan VPN kita seolah-olah membuat jaringan didalam jaringan atau biasa disebut tunnel. VPN menggunakan salah satu dari tiga teknologi tunneling yang ada yaitu: PPTP, L2TP dan standar terbaru, Internet Protocol Security (biasa disingkat menjadi IPSec). VPN merupakan perpaduan antara teknologi tunneling dan enkripsi.

2.2 Tahap Identifikasi (Identification)

Indikator awal bahwa terjadi serangan pada jaringan adalah mencakup kinerja jaringan yang buruk, layanan tidak dapat diakses atau sistem crash.Kemampuan untuk mengidentifikasi dan memahami sifat dari serangan dan target akan membantu dalam proses penahanan dan pemulihan. Untuk tujuan ini, organisasi memerlukan alat yang memberikan visibilitas terhadapinfrastruktur teknologi informasi yang mereka kelola. Sebelum serangan terjadi pada jaringan, pengintaian dari target dilakukan oleh penyerang, termasuk pemindaian kerentanan yang terdapat pada jaringan target, kerentanan dapat diketahui dengan cara

mengirimkan paket cacat ke host target untuk menganalisis perubahan dalam tenggang waktu respon tertentu. Kegiatan pengintaian ini mungkin sulit untuk dideteksi, terutama karena dapat terjadi sebelum serangan terjadi. Seorang penyerang juga memiliki pengetahuan untuk memastikan pemindaian lalu lintas tidak melewati ambang batas yang diperlukan untuk memicu alarm dari alat monitor jaringan. Namun, ada kemungkinan tersedia teknik intelijen yang menunjukkan kemungkinan peningkatan serangan terhadap jaringan komputer suatu organisasi.

Langkah-langkah yang bisa diambil pada tahap ini,

a. Menentukan apakah jaringan organisasi merupakan target utama atau korban dari imbas (misal: imbas dari serangan terhadap penyedia layanan internet atau penyedia hosting?). Beberapa indikasi yang dapat dijadikan untuk melakukan identifikasi terhadap serangan pada jaringan adalah
    - Melambatnya lalu-lintas jaringan
    - Melambatnya proses pada komputer client
    - Penggunaan ruang disk yang bertambah
    - Waktu login yang lama, bahkan ditolak
    - Perubahan pada beberapa password
    - Log penuh
    - Anomali pada fungsi port
b. Memahami aliran logis dari serangan.
c. Menentukan jenis lalu lintas yang sedang digunakan, seperti alamat IP, port dan protokol.
d. Mempertimbangkan untuk menggunakan alat analisis jaringan untuk menentukan jenis lalu lintas yang digunakan dalam serangan itu (misalnya, tcpdump, wireshark, Snort).
e. Me-review log yang tersedia untuk memahami serangan dan apa yang menjadi sasaran.
f. Memberitahu personil yang tepat, ini mungkin termasuk manajemen senior dan tim hukum
g. Mengidentifikasi aset dan layanan pada jaringan yang masih dapat diberikan oleh organisasi.
h. Mengidentifikasi apakah seluruh perangkat lunak selalu up to date dengan patch terbaru?

i. Apakah pada jaringan menjalankan layanan yang tidak perlu seperti Telnet atau FTP?
j. Menonaktifkan semua lalu lintas yang jelas palsu (misalnya, alamat IP internal yang seharusnya tidak boleh masuk atau keluar dari jaringan Anda). Menerapkan daftar blok Bogon (ruang alamat yang tidak dialokasikan) pada batas jaringan.
k. Menetapkan prosedur tentang cara untuk memisahkan jaringan yang satu dengan jaringan yang lain apabila terjadi serangan pada suatu jaringan. Sementara, menggunakan perangkat jaringan yang ada, seperti router dan switch terkelola untuk mempertahankan terhadap serangan jaringan. Sedapat mungkin menerapkan penyaringan layanan pada router terluar untuk mengurangi beban pada perangkat keamanan seperti firewall.
l. Menonaktifkan semua layanan yang tidak perlu dan membatasi akses ke dan dari semua host kritis, berdasarkan karakteristik lalu lintas jaringan normal.
m. Memahami perilaku "normal" dari lalu lintas jaringan, penggunaan CPU, sambungan dan penggunaan memori dari host dalam kondisi normal sehingga alat monitoring jaringan akan memicu peringatan pada perubahan abnormal.
n. Menentukan dampak dari tingkat keparahan yang terjadi

2.3 Tahap Penahanan (Containment)

Memiliki rencana penahanan yang telah ditentukan sebelum serangan untuk sejumlah skenario secara signifikan akan meningkatkan kecepatan respon dan kerusakan akibat serangan pada jaringan. Sebagai contoh, strategi penahanan untuk sebuah mail server mungkin berbeda dari satu untuk server web. Meremehkan pentingnya fase ini dapat menyebabkan kesalahan dan kerusakan yang signifikan.

Oleh karena itu, memahami sifat serangan pada jaringan dan mendokumentasikan terkait proses pengambilan keputusan sangat penting. Suatu organisasi harus secara jelas mengidentifikasi perimeter

dari jaringan dan aset yang terkena serangan. Load balancers, teknologi modern firewall (Deep Packet Inspection, proxy, penyaringan lapisan aplikasi), konten dari caching, layanan dinamis DNS adalah beberapa alat organisasi yang dapat memanfaatkan untuk menampung serangan pada jaringan yang sedang berlangsung menyerang.

a. Tidak melakukan perubahan/modifikasi pada sistem

b. Menghubungi ISP untuk meminta penerapan penyaringan.

c. Jika memungkinkan, memblokir lalu lintas yang dekat dengan cloud jaringan (router, firewall, load balancer, dll).

d. Merelokasi target ke alamat IP lain jika suatu host tertentu sedang ditargetkan. Ini adalah solusi sementara.

e. Jika aplikasi tertentu sedang ditargetkan, pertimbangkan untuk menonaktifkan sementara.

f. Mengidentifikasi dan memperbaiki kerentanan atau kelemahan yang tereksploitasi. Sebagai contoh, misalnya layanan tidak terpakai yang sengaja diaktifkan dan tertinggal pada perangkat untuk melayani public atau sistem operasi yang tidak dipatched.

g. Melakukan penyaringan berdasarkan karakteristik serangan, salah satu contohnya adalah memblokir paket echo ICMP.

h. Menerapkan rate limiting untuk protokol tertentu, mengijinkan dan membatasi jumlah paket per detik untuk protokol tertentu mengakses suatu host.

i. Mengidentifikasi lokasi dan/atau pemilik sistem yang terlibat dalam insiden tersebut dengan memeriksa hal-hal berikut :

    i. Tabel ARP jaringan untuk memetakan alamat IP ke alamat MAC

ii. Catatan log DHCP untuk alamat MAC dan hostname
iii. Perintah "nbtscan" untuk query informasi pada master NetBIOS
iv. Sistem kontrol jaringan untuk semua komputer yang digunakan
v. Perangkat lunak manajemen jaringan (radius)
vi. Sistem manajemen log file (misal ‘Qradar’)

j. Menentukan apakah komputer yang telah diblokir masih memiliki akses jaringan. Jika demikian, hal ini dapat dicapai dalam beberapa cara oleh tim jaringan:

i. Pemeriksaan pada port switch , interface router , perimeter jaringan
ii. Memblokir alamat MAC pada semua jaringan nirkabel
iii. Menonaktifkan akses dial-up modem
iv. Nonaktifkan akses VPN

k. Daftar komputer yang telah diblokir harus diumumkan ke semua anggota organisasi. Prosedur untuk memblokir/membuka blokir komputer yang telah terserang harus tersedia.Sebuah alternatif untuk memblokir semua akses jaringan, jika tersedia bisa berfungsi untuk menempatkan computer dalam jaringan yang dikarantina.

l. Mungkin ada kasus ketika sebuah protokol (TCP/UDP) atau port tertentu perlu diblokir pada perimeter jaringan beberapa antarmuka jaringan lainnya untuk mencegah penyebaran.

m. Memberi tahu kepada administrator sistem dan/atau pengguna yang bertanggung jawab atas sistem.

n. Mengisolasi komputer yang terkena dampak, baik dengan cara mencabut kabel jaringan (lebih disukai) atau mematikan komputer. Mencabut kabel jaringan dan membiarkan komputer masih nyala, merupakan cara yang terbaik karena dengan cara

shutdown dapat mengubah atau menghancurkan bukti, seperti infeksi malware pada memori. Bisa dilakukan (mematikan komputer) apabila memory telah dicopy untuk proses forensic (optional).

- Melakukan analisa digital forensik.

2.4 Tahap Eradication

Tahap eradication merupakan tahap untuk melakukan analisa lebih dalam terhadap barang bukti yang telah ditahan, pada tahap ini dilakukan proses analisa terhadap beberapa log file yang terdapat pada server, peralatan aktif jaringan, IDS, Firewall, sistem file, dan aplikasi. Pada tahap ini dilakukan analisa forensik dari barang bukti. Keberhasilan proses forensik sangat ditentukan oleh kualitas dan kuantitas informasi yang terkumpul. Log file dapat merupakan sumber informasi yang penting bagi proses forensik. Log file mengandung informasi tentang berbagai sumber daya sistem, proses-proses dan aktivitas pengguna. Protocol analyzer, sniffer, server SMTP, DHCP, FTP dan WWW, router, firewall dan hampir semua aktivitas sistem atau user dapat dikumpulkan dalam log file. Tetapi jika administrator sistem tidak dapat mencatat, maka fakta yang diperlukan untuk menghubungkan pelaku dengan insiden tidak ada. Sayangnya penyerang dan penjahat yang pintar mengetahui hal ini dan tujuan pertamanya adalah merusak atau mengubah log file untuk menyembunyikan aktivitas mereka. Hal kedua yang penting tetapi sering dilupakan adalah sistem clock. Pencatatan suatu file berhubungan dengan time stamp dan date stamp yang memungkinkan analis forensik untuk menentukan urutan kejadian. Tetapi jika sistem clock tidak dikoreksi/dikalibrasi secara berkala dapat dimatikan dari mana saja dari beberapa detik sampai beberapa jam. Hal ini menyebabkan masalah karena korelasi antara log file dari komputer yang berbeda.Sistem clock yang berbeda akan menyulitkan bahkan tidak mungkin mengkorelasikan kejadian. Solusi yang sederhana untuk mensinkronisasi clock adalah seluruh server dan sistem berjalan pada

suatu daemon seperti UNIX ntpd daemon, waktu dan tanggal sistem secara berkala harus disinkronisasikan dengan suatu atomic clock yang disediakan pemerintah.

2.5. Recovery

Tergantung pada strategi kerja pada tahap penahanan dan kepekaan terhadap dampak yang diakibatkan, organisasi mungkin berada pada tekanan yang berbeda untuk pulih dari serangan jaringan. Memahami karakteristik serangan diperlukan untuk pemulihan yang cepat dan tepat.

a. Konfirmasikan bahwa serangan pada jaringan telah selesai dan layanan bisa dilakukan kembali
b. Konfirmasikan bahwa jaringan telah kembali ke kinerja semula.
c. Jika perlu, melakukan patch dan memperbarui semua mesin yang terkena dampak.
d. Jika sumber serangan teridentifikasi berasal dari luar jaringan, meminta bantuan dari ISP merupakan cara yang paling tepat. Sumber serangan yang berasal dari luar jaringan (dari internet) bisa dihentikan dengan meminta ISP untuk melakukan blokir terhadap lalulintas data dari sumber serangan menuju jaringan.
e. Melakukan ulasan dan monitoring terhadap log untuk melihat adanya tanda-tanda pengintaian. Melindungi dan menjaga log untuk kebutuhan penegakan hukum di masa depan.
f. Melakukan pemulihan dari back up sistem yang masih baik.

2.6 Tahap Follow up

Tahap dimana semua tahap sebelumnya telah dilalui, tujuan dari tahap ini adalah untuk,

a. Pelaporan, membuat laporan mengenai langkah-langkah dan hasil yang telah didapatkan pada penanganan insiden yang telah

dilakukan. Mendokumentasikan dampak dan biaya dari terjadinya insiden serangan pada jaringan.

b. Pembelajaran, adalah langkah yang sangat penting yang sering diabaikan. Pelajaran harus dapat dipetik dari kegiatan sesegera mungkin setelah penanganan insiden usai. Semua keputusan dan langkah-langkah yang diambil sepanjang siklus penanganan insiden harus ditinjau. Semua prosedur harus ditinjau untuk melihat di mana perbaikan dapat dilakukan.

c. Peningkatan kepedulian terhadap keamanan jaringan, dengan melakukan review setelah setiap kejadian, akan memungkinkan bagi organisasi untuk melakukan perbaikan terus-menerus dan berpotensi pada pengurangan yang signifikan akibat dampak insiden.

d. Memungkinan pembaharuan pada dokumen-dokumen berikut:

- Standard Operating Procedures
- Prosedur Operasi Darurat
- Disaster Recovery Plan (DRP)

LAMPIRAN A - Informatif

Serangan pada jaringan

Gambar 2.

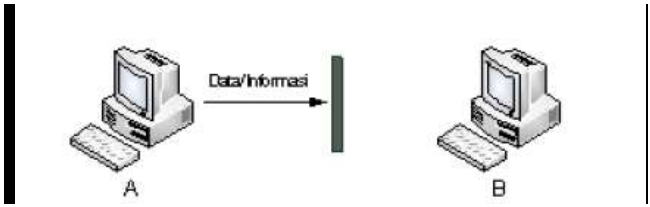
Pertukaran Informasi normal

Serangan adalah sesuatu yang telah mengganggu/merusak kinerja dari sebuah sistem. Idealnya , sebuah pertukaran informasi di dalam sistem jaringan computer dapat digambarkan seperti pada gambar diatas. Informasi dari user A diterima secara utuh oleh user B tanpa ada perubahan, penyadapan atau modifikasi terhadap pesan.

Namun, dengan adanya serangan terhadap keamanan jaringan komputer, pesan yang dikirimkan dapat diambil alih oleh pihak ketiga untuk kemudian dimodifikasi atau dibuat pesan palsu, atau pesan tidak sampai sama sekali. Serangan ini mempunyai 2 sifat yaitu pasif dan aktif. Serangan yang bersifat pasif adalah serangan yang tidak merusak ataupun merubah pesan yang dikirimkan, sedangkan serangan yang bersifat aktif adalah serangan yang merusak atau adanya usaha modifikasi terhadap pesan maupun resource sistem. Tujuan dari serangan yang bersifat pasif adalah memperoleh informasi yang sedang ditransmisikan. Sebagai contoh: penyadapan terhadap saluran telepon, analisa lalu lintas data di dalam jaringan, penangkapan pesan, dan lain-lain. Serangan pada jaringan dapat dilakukan dengan menggunakan teknik-teknik sebagai berikut :

1. Interupsi

Serangan dengan bentuk interupsi artinya mencegah agar user B tidak dapat menerima informasi yang dikirim oleh user A. Pesan yang dikirimkan oleh user A dihalangi oleh penyerang sehingga tidak sampai ke user B.

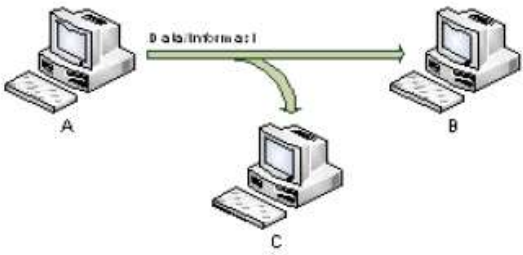


Gambar 3.
Gambaran interupsi

Contoh dari serangan ini adalah :
Denial of Service atau yang mungkin lebih sering kita dengar dengan nama DoS merupakan suatu aktifitas yang menghambat laju kerja dari sebuah layanan atau malah mematikannya sehingga dapat menyebabkan pengguna yang asli tidak dapat menggunakan layanan. Serangan ini dapat mengakibatkan terhambatnya aktifitas yang akan dilakukan oleh korban yang akibatnya boleh dibilang sangat fatal. DoS merupakan serangan yang cukup menakutkan di sistem jaringan karena akibat dari serangan ini server akan mati dan tidak dapat beroperasi lagi sehingga otomatis tidak dapat memberikan pelayanan lagi.
Denial of Service (DoS) merupakan serangan yang melakukan ekploitasi aspek dari suite Internet Protocol untuk menghalangi akses pihak yang berhak atas informasi atau sistem yang diserang. Serangan ini biasanya memanfaatkan hole(celah keamanan) pada sistem operasi yang dipergunakan. Hole yang memungkinkan DoS, berada dalam kategori C, yang berada dalam prioritas rendah. Hole ini berada di dalam bagian jaringan dari sistem operasi itu sendiri. Ketika hole macam ini muncul, hole ini harus diperbaiki oleh pemilik software tersebut atau di-patch oleh vendor yang mengeluarkan sistem operasi tersebut. Contoh dari serangan ini adalah TCP SYN dimana permintaan koneksi jaringan dikirimkan ke server dalam jumlah yang sangat besar. Akibatnya server dibanjiri permintaan koneksi dan menjadi lambat atau bahkan tidak dapat dicapai sama sekali. Hole ini terdapat nyaris di semua sistem operasi yang menjalankan TCP/IP untuk berkomunikasi di internet. Hal ini tampaknya menjadi masalah yang terdapat di dalam desain suite TCP/IP,

dan merupakan sesuatu yang tidak mudah diselesaikan. Antisipasi serangan ini dengan menggunakan firewall, backup dan redundancy, dan Intrusion Detection System.

2. Intersepsi



Gambar 4.
Gambaran Intersepsi

Intersepsi adalah bentuk serangan dimana pihak ketiga menangkap pesan yang dikirimkan oleh user A tetapi pesan tersebut tetap dapat diterima oleh user B secara utuh. Contoh dari serangan ini adalah Password Sniffing. Pada serangan ini seolah- olah ada seorang attacker yang berada diantara korban dan server. Attacker akan melancarkan sniffing terhadap paket-paket data, sehingga bisa mendapatkan password dari korban.

Packet Sniffing adalah sebuah metode serangan dengan cara mendengarkan seluruh paket yang lewat pada sebuah media komunikasi, baik itu media kabel maupun radio. Setelah paket-paket yang lewat itu didapatkan, paket-paket tersebut kemudian disusun ulang sehingga data yang dikirimkan oleh sebuah pihak dapat dicuri oleh pihak yang tidak berwenang. Hal ini dapat dilakukan karena pada dasarnya semua koneksi ethernet adalah koneksi yang bersifat broadcast, di mana semua host dalam sebuah kelompok jaringan akan menerima paket yang dikirimkan oleh sebuah host. Pada keadaan normal, hanya host yang menjadi tujuan paket yang akan memproses paket tersebut sedangkan host yang lainnya akan mengacuhkan paket-paket tersebut. Namun pada keadaan tertentu, sebuah host bisa merubah konfigurasi sehingga host

tersebut akan memproses semua paket yang dikirimkan oleh host lainnya. Cukup sulit untuk melindungi diri dari gangguan ini karena sifat dari packet sniffing yang merupakan metode pasif (pihak penyerang tidak perlu melakukan apapun, hanya perlu mendengar saja). Namun ada beberapa hal yang bisa dilakukan untuk mengatasi hal ini, yaitu:

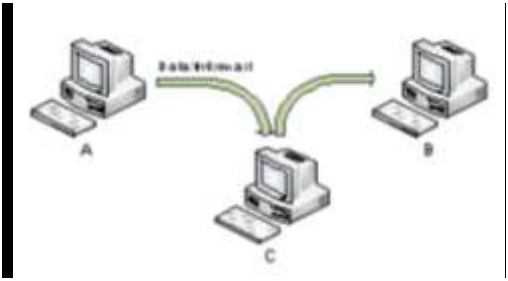
a. Secara rutin melakukan pemeriksaan apakah ada host di jaringan kita yang sedang dalam mode promiscuous, yaitu sebuah mode dimana host tersebut akan memproses semua paket yang diterima dari media fisik. Akan tetapi hal ini hanya akan melindungi diri kita terhadap packet sniffer yang berada pada satu kelompok jaringan dengan kita. Penyerang yang melakukan sniffing dari luar jaringan komputer kita tidak akan terdeteksi dengan menggunakan metode ini.

b. Mempergunakan teknologi enkripsi dalam melakukan pengiriman data. Ini tidak akan mencegah packet sniffer untuk mencuri paket yang dikirimkan, akan tetapi paket - paket yang dicuri tidak bisa dipergunakan karena dikirimkan dengan menggunakan format yang terenkripsi.

c. Melakukan koneksi VPN, sehingga tetap bisa mempergunakan aplikasi yang tidak mendukung SSL atau TLS dengan aman.

Packet Sniffing sebagai tools pengelola jaringan Sebenarnya selain sebagai menjadi alat untuk melakukan kejahatan, packet sniffer juga bisa digunakan sebagai alat pertahanan. Dengan melakukan analisa paket-paket yang melalui sebuah media jaringan komputer, pengelola dapat mengetahui apabila ada sebuah host yang mengirimkan paket-paket yang tidak normal, misalnya karena terinfeksi virus. Sebuah IDS juga pada dasarnya adalah sebuah packet sniffer yang bertugas untuk mencari host yang mengirimkan paket-paket yang berbahaya bagi keamanan. Selain itu packet sniffer juga bisa menjadi alat untuk melakukan analisa permasalahan yang sedang dihadapi sebuah jaringan komputer. Misalkan ketika sebuah host tidak dapat berhubungan dengan host lainnya yang berada pada kelompok jaringan yang berbeda, maka dengan packet sniffer, pengelola jaringan komputer dapat melakukan penelusuran dimana permasalahan koneksi itu terletak.

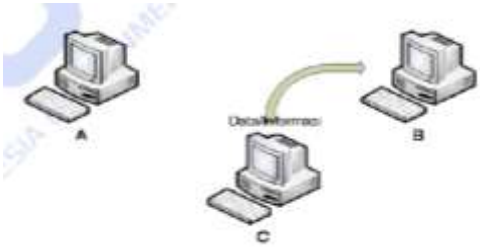
3. Modifikasi



Gambar 5.
Gambaran Modifikasi

Modifikasi adalah suatu bentuk penangkapan pesan dan disertai dengan modifikasi atau usaha untuk merubah pesan tersebut kemudian dikirimkan ke user yang sebenarnya. Contoh serangan ini adalah serangan oleh virus Trojan horse, TCP Hijacking.
Trojan horse merupakan program yang terselubung dan bisa menempel dalam e-mail seseorang. Trojan horse bisanya program yang berbentuk sesuatu yang sangat menarik, sehingga seseorang menginginkan program tersebut untuk memilikinya. Apabila Trojan horse telah masuk ke dalam sistem seseorang maka program tersebut akan memberikan akses secara keseluruhan terhadap sistem yang telah terinfeksi tersebut. Trojan horse biasanya dibuat untuk mendapatkan akses ke file sistem orang lain. Dengan demikian penyerang mampu melakukan pencurian file dan password, merusak file, atau memonitor apa yang dilakukan korbannya, mendownload file, menonaktifkan perangkat keras tertentu, merubah nama file, melakukan force shut down atau reboot. Antisipasi serangan virus dengan anti virus yang selalu terupdate. TCP Hijacking bekerja berdasarkan pada IP Spoofing dan prediksi teradap nomor sequence dari paket TCP. Tujuannya adalah untuk mengambil seluruh paket TCP. Aplikasi-aplikasi yang menggunakan TCP antara lain adalah Telnet, rLogin, FTP. Dari aksi TCP Hijacking ini seorang penyerang bisa mendapatkan ID dan password dari korban. Antisipasi TCP Hijacking dengan Static ARP Tables dan Enkripsi data.

4. Fabrikasi



Gambar 6.
Gambaran Fabrikasi

Fabrikasi adalah usaha penyerang untuk memberikan pesan palsu kepada user lain. Contoh dari serangan ini adalah packet spoofing. Packet Spoofing adalah sebuah model serangan yang bertujuan untuk menipu seseorang. Serangan ini dilakukan dengan cara mengubah alamat asal sebuah paket, sehingga dapat melewati perlindungan firewall dan menipu host penerima data. Hal ini dapat dilakukan karena pada dasarnya alamat IP asal sebuah paket dituliskan oleh sistem operasi host yang mengirimkan paket tersebut. Dengan melakukan raw-socket-programming, seseorang dapat menuliskan isi paket yang akan dikirimkan setiap bit-nya sehingga untuk melakukan pemalsuan data dapat dilakukan dengan mudah.
Salah satu bentuk serangan yang memanfaatkan metode IP Spoofing adalah 'man-in-the-middle-attack'. Pada serangan ini, penyerang akan berperan sebagai orang ditengah antara dua pihak yang sedang berkomunikasi. Misalkan ada dua pihak yaitu pihak A dan pihak B lalu ada penyerang yaitu C. Setiap kali A mengirimkan data ke B, data tersebut akan dicegat oleh C, lalu C akan mengirimkan data buatannya sendiri ke B, dengan menyamar sebagi A. Paket balasan dari B ke A juga dicegat oleh C yang kemudian kembali mengirimkan data 'balasan' buatannya sendiri ke A. Dengan cara ini, C akan mendapatkan seluruh data yang dikirimkan antara A dan B, tanpa diketahui oleh A maupun C. Untuk mengatasi serangan yang berdasarkan IP Spoofing, sebuah sistem operasi harus dapat memberikan nomor-urut yang acak ketika menjawab inisiasi koneksi dari sebuah host. Dengan nomor urut paket yang acak, akan sangat sulit bagi seorang penyerang untuk dapat melakukan pembajakan transmisi data. Untuk mengatasi model serangan 'man-in-the-middle-attack', perlu ada sebuah metode untuk melakukan

otentikasi host yang kita hubungi. Otentikasi dapat berupa digital-certificate yang eksklusif dimiliki oleh host tersebut. Konfigurasi firewall yan tepat juga dapat meningkatkan kemampuan jaringan komputer dalam menghadapi IP Spoofing. Firewall harus dibuat agar dapat menolak paket-paket dengan alamat IP sumber jaringan internal yang masuk dari interface yang terhubung dengan jaringan eksternal Tindakan Pengamanan Jaringan Pada bagian ini akan diuraikan beberapa pengamanan terhadap sistem jaringan, dimulai dari bagian yang berhubungan dengan perimeter terluar sampai dengan client yang berhubungan langsung dengan jaringan.

Otentikasi

Otentikasi berarti seseorang yang akan menggunakan sistem harus menunjukkan jatidirinya. Identifikasi pemakai saat login merupakan dasar asumsi sistem proteksi sehingga metode otentifikasi didasarkan pada tiga cara, yaitu sesuatu yang diketahui pemakai, yang dimiliki pemakai, dan mengenai pemakai. Password merupakan salah satu otentifikasi yang diketahui pemakai, dimana pemakai memilih suatu kata kode, mengingatnya dan mengetikkannya saat akan mengakses sistem komputer. Teknik pengamanan dengan password mempunyai beberapa kelemahan, terutama karena pemakai sering memilih password yang mudah diingatnya. Supaya password relatif aman, maka diperlukan suatu aturan tentang password seperti sebagai berikut

Account Locking

Jika ada user yang melakukan kesalahan login beberapa kali melebihi dengan yang sudah ditentukan, maka server secara otomatis akan melakukan locking terhadap account tersebut. Administrator akan menentukan jumlah batas percobaan kesalahan melakukan login, dan lamanya account akan di-locking. Namun administrator juga dapat melakukan locking terhadap account tertentu secara langsung. Locking dengan cara ini, tidak dapat dilakukan unlocking secara otomatis.

Password Aging & Expiration

Administrator dapat menentukan masa berlakunya penggunaan password. Bila masa berlakunya sudah lewat, maka user tersebut atau administratornya harus mengubah password tersebut. Administrator juga dapat menentukan grace period, yaitu tenggang waktu yang diberikan

kepada user untuk mengganti passwordnya. Bila passwordnya belum diganti hingga grace period berakhir, maka accountnya akan hangus dan user tersebut tidak dapat lagi melakukan login. Administrator juga dapat menentukan interval waktu di mana password yang sudah expired tidak dapat digunakan lagi secara langsung.

Password Complexity Verification

Password complexity verification dapat dispesifikasi menggunakan PL/SQL yang akan mengatur parameter profil default. Password complexity verification akan melakukan pemeriksaan-pemeriksaan berikut:

- password memiliki panjang minimum 4;
- password tidak sama dengan user ID;
- password sedikitnya memiliki satu alfabetik, satu numerik, dan satu tanda baca;
- password tidak boleh sama dengan kata-kata sederhana seperti welcome, account, database, atau user;

Password dimaksudkan untuk memberi identitas yang unik ke tiap user. Oleh karena itu, ia harus bersifat rahasia atau hanya diketahui oleh user yang bersangkutan. Namun seringkali user berperilaku sehingga passwordnya dapat diketahui oleh orang lain. Perilaku itu misalnya :

− memilih password yang mudah ditebak sehingga tidak benar-benar rahasia

− memberitahu passwordnya ke teman, rekan kerja, atau anggota keluarga

− menulis passwordnya dan meletakkannya di dekat komputer atau di tempat yang privat seperti dompet.

Otorisasi

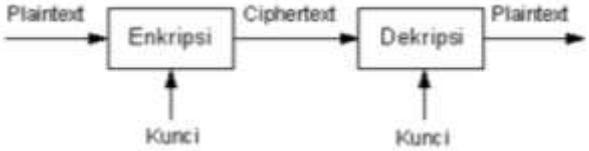
Otorisasi adalah pemberian hak akses terhadap suatu resource kepada seseorang. Pembatasan dapat dilakukan untuk memperkecil peluang penembusan oleh pemakai yang tidak diotorisasi. Metode domain controller pada setiap user yang login dapat diterapkan terhadap sistem. Dengan diterapkannya metode ini diharapkan akses user terhadap data-data dapat dibatasi sesuai dengan hak aksesnya. Otorisasi juga harus mengatur pembatasan login, misalnya dengan login pada terminal dan waktu tertentu Atau dengan metode call back, yaitu login dapat dilakukan oleh siapapun tetapi setelah sukses maka sistem akan segera

memutuskan koneksi dan memanggil nomor telepon yang telah disepakati. Acces-Control-Lists menentukan siapa yang diberikan akses ke sistem atau jaringan komputer lokal atau remote, dan juga informasi apa saja dan berapa banyak seseorang dapat menerima. Sumber-sumber informasi yang berhubungan dalam jaringan dapat diorganisasikan dalam sebuah bentuk hierarki, dan Access-Control-Lists dapat juga menetapkan akses utuk pengguna-pengguna tertentu dan grup-grup pengguna tertentu.
Sebagai tambahan, mekanisme-mekanisme kendali akses dapat didistribusikan pada jaringan. Mekanisme-mekanisme tidak harus teletak pada host yang sama sebagaimana website. Ini berarti para administrator secara fisik dapat menjalankan servis-servis kendali akses pada sebuah host yang terpisah, memungkinkan banyak website menggunakan mekanisme-mekanisme kendali akses yang sama. Menggunakan metode Single Sign On, Sebuah on-line servis berbasis web untuk registrasi dan mengatur user dan servis-servis yang aman. Salah satu prinsip dasar Single Sign On adalah kesamaan user name dan password pada berbagai aplikasi, misalnya antara Active Directory/File Server, Zimbra Mail Server, Squid Proxy Server dan aplikasi web server. Single Sign On dapat ditempuh dengan menggunakan LDAP sebagai database penyimpanan user name dan password.

Enkripsi

Salah satu hal yang penting dalam komunikasi pada intranet agar kerahasian data terjamin adalah enkripsi. Enkripsi adalah sebuah proses yang melakukan perubahan sebuah kode dari yang bisa dimengerti menjadi sebuah kode yang tidak bias dimengerti (tidak terbaca). Enkripsi merupakan cara untuk melindungi data atau informasi yang akan dikirimkan melalui media komunikasi. Untuk melindungi data atau informasi yang akan dikirim, perubahan harus dilakukan pada data atau informasi tersebut. Pada data atau informasi yang dikirim harus dilakukan enkripsi yang biasanya merupakan persamaan matematik. Biasanya kedua persamaan matematik (untuk enkripsi dan dekripsi) tersebut memiliki hubungan matematis yang cukup erat.
Proses yang dilakukan untuk mengamankan sebuah pesan (yang disebut plaintext) menjadi pesan yang tersembunyi (disebut ciphertext) adalah enkripsi (encryption). Enkripsi digunakan untuk menyandikan data-data atau informasi sehingga tidak dapat dibaca oleh orang yang tidak berhak. Dengan enkripsi data atau informasi disandikan (encrypted) dengan menggunakan sebuah kunci (key). Untuk membuka (decrypt) data

tersebut digunakan juga sebuah kunci yang dapat sama dengan kunci untuk mengenkripsi (untuk kasus private key cryptography) atau dengan kunci yang berbeda (untuk kasus public key cryptography). Ciphertext adalah pesan yang sudah tidak dapat dibaca dengan mudah. Menurut ISO 7498-2, terminologi yang lebih tepat digunakan adalah “encipher”. Proses sebaliknya, untuk mengubah ciphertext menjadi plaintext, disebut Dekripsi (decryption). Menurut ISO 7498-2, terminology yang lebih tepat untuk proses ini adalah “decipher”.



Gambar 7.
Ilustrasi enkripsi deskripsi

Karakteristik cryptosytem yang baik sebagai berikut :

1.Keamanan sistem terletak pada kerahasiaan kunci dan bukan pada kerahasiaan algoritma yang digunakan.
2. Cryptosystem yang baik memiliki ruang kunci (keyspace) yang besar.
3. Cryptosystem yang baik akan menghasilkan ciphertext yang terlihat acak dalam seluruh tes statistik yang dilakukan terhadapnya.

Berdasarkan persamaan kunci yang digunakan untuk proses enskripsi dan deskripsi, maka Chryptosistem dapat dibedakan menjadi 2 yaitu,
A. Symmetric Cryptosystem
Dalam symmetric cryptosystem ini, kunci yang digunakan untuk proses enkripsi dan dekripsi pada prinsipnya identik, tetapi satu buah kunci dapat pula diturunkan dari kunci yang lainnya. Kunci-kunci ini harus dirahasiakan. Oleh karena itulah sistem ini sering disebut sebagai secret-key ciphersystem. Contoh dari sistem ini adalah Data Encryption Standard (DES), Blowfish, IDEA.

B. Assymmetric Cryptosystem

Dalam asymmetric cryptosystem ini digunakan dua buah kunci. Satu kunci yang disebut kunci publik (public key) yang dapat dipublikasikan,

sedang kunci yang lain yang disebut kunci privat (private key) yang harus dirahasiakan. Proses menggunakan sistem ini dapat diterangkan secara sederhana sebagai berikut : bila A ingin mengirimkan pesan kepada B, A dapat menyandikan pesannya dengan menggunakan kunci publik B, dan bila B ingin membaca surat tersebut, ia perlu mendekripsikan surat itu dengan kunci privatnya. Dengan demikian kedua belah pihak dapat menjamin asal surat serta keaslian surat tersebut, karena adanya mekanisme ini. Contoh sistem ini antara lain RSA Scheme dan Merkle-Hellman Scheme.

Semua Data/informasi yang keluar atau masuk menuju jaringan harus dienkripsi supaya jika data/informasi jatuh ke pihak yang tidak diinginkan, akan sulit untuk dibaca. Usaha-usaha penyadapan proses penyampain e-mail melalui Internet semakin hari semakin meluas. Terlebih setelah masuknya transaksi dunia bisnis ke dunia Internet yang tentunya memerlukan tingkat kerahasiaan tertentu. Jika menginginkan privacy dan keamanan saat mengirimkan file-file maupun e-mail, proses enkripsi menjadi salah satu solusi utama. PGP (Pretty Good Privacy) adalah program enkripsi yang memiliki tingkat keamanan cukup tinggi dengan menggunakan “private-public key” sebagai dasar autentifikasinya. Program PGP yang dibuat oleh Phill Zimmermann ini memiliki 2 versi yaitu “USA version” dan “International version”. PGP versi USA hanya bias digunakan di wilayah USA dan oleh warganegara USA saja. Versi USA ini menggunakan algoritma RSA (yang telah menjadi hak paten) dalam enkripsinya. Sedangkan versi International menggunakan algoritma MPILIB yang diciptakan khusus oleh Phill Zimmermann sendiri. PGP versi Internasional bisa digunakan oleh seluruh orang di dunia. Sebagai pembeda, PGP versi Internasional membubuhkan akhiran ‘i’ pada nomor versi PGP. Sebagai contoh, nomor versi PGP terakhir adalah 7.0.3 untuk USA version dan 7.0.3i untuk International version. Beberapa tahun belakangan ini, penggemar dan pengguna PGP semakin meningkat sehingga PGP telah menjadi standar de-facto program enkripsi untuk electronic mail Program PGP “International version” merupakan shareware dan dapat didownload dari beberapa ftp server sebagai berikut :

- ftp://ftp.ifi.uio.no/pub/pgp/ (primary)
- ftp://ftp.ox.ac.uk/pub/crypto/pgp/
- ftp://ftp.dsi.unimi.it/pub/security/crypt/PGP/
- ftp://ftp.informatik.uni-hamburg.de/pub/virus/crypt/pgp/

Program PGP tersedia dalam berbagai platform seperti MS-Dos, Macintosh, Unix, VMS, OS/2, Atari, dlsb. Untuk platform MS-Dos sendiri, terdapat dua jenis yaitu pgp263i.zip (16 bit) dan pgp263ix.zip (32 bit).

Untuk versi 32 bit, terdapat perbedaan pada kecepatan proses enkripsi dan pembuatan key dibandingkan dengan versi 16 bit. Seperti yang telah disinggung di awal makalah, PGP menggunakan “private-public keys” sebagai dasar otorisasinya. Setiap kali kita membuat kunci, PGP akan menciptakan dua buah kunci yaitu Private key dan Public key yang merupakan sebuah pasangan yang bersesuaian. Private key adalah kunci yang hanya diketahui oleh kita sendiri. Public key adalah kunci yang kita beritahukan kepada orang-orang yang kita percaya. Public key digunakan sebagai dasar proses pengenkripsian dokumen-dokumen yang hanya bisa dibuka oleh orang yang memiliki private key yang bersesuaian.

Tanda Tangan dan Sertifikat Digital

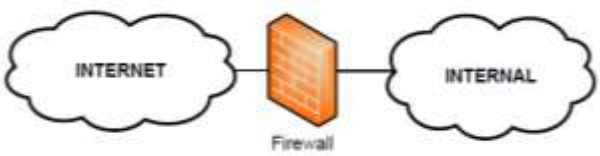
Tanda tangan digital (digital signature) merupakan autentikasi elektronik yang tidak dapat dipalsukan. Teknik ini memastikan bahwa pesan atau dokumen dikirim berasal dari pengirim yang sah, dan bahwa pesan itu tidak bisa diubah setelah dokumen itu ditandatangani. Tujuan dari tanda tangan digital adalah untuk mendeteksi adanya modifikasi data yang tidak diotorisasi dan untuk mengotentikasi identitas dari penandatangan. Fungsi-fungsi ini dicapai dengan menggenerate blok data yang biasanya ukurannya lebih kecil dari data asli. Blok data yang lebih kecil ini dibubuhkan pada data asli dan pada identitas pengirim. Untuk menghasilkan tanda tangan digital, program sinyal digital melewatkan file untuk dikirimkan melalui fungsi hash satu arah. Setelah message digest dihitung, kemudian dienkripsi dengan kunci privat pengirim. Penerima kemudian mendekripsi message digest dengan menggunakan kunci publik pengirim. Jika kunci publik ini membuka message digest dan benar bahwa ia merupakan kunci publik pengirim, verifikasi pengirim telah tercapai. Verifikasi terjadi karena hanya kunci public pengirim yang dapat mendekrip message digest yang dienkripsi dengan kunci privat pengirim. Kemudian, penerima dapat menghitung message digest dari file yang diterima menggunakan fungsi hash yang identik dengan pengirim. Jika message digest identik dengan message digest yang dikirim sebagai bagian dari tanda tangan, maka pesan tidak dimodifikasi. Proses di atas membuktikan bahwa pesan yang diterima memang dikirimkan oleh pengirim dan tidak diubah selama pengiriman pesan. Namun demikian, proses ini tidak membuktikan bahwa pengirimnya adalah orang yang mengklaim mengirim pesan itu. Pengirim tersebut bisa saja seorang penyamar. Untuk memverifikasi identitas pengirim diperlukan sebuah sertifikat digital (digital certificate), yang dikeluarkan oleh pihak ketiga

yang dipercaya, yang disebut otoritas sertifikasi (certification authority-CA). Sebuah sertifikat digital digunakan dalam hubungannya dengan sebuah sistem enkripsi kunci publik untuk membuktikan keaslian (otentikasi pengirim pesan). Proses sertifikasi ini bervariasi, bergantung pada tingkat sertifikasi yang diinginkan. Ini melibatkan pembentukan identitas seseorang dengan dokumen resmi, seperti surat izin mengemudi, pengesahan dengan notaris, dan sidik jari, serta pembuktikan kepemilikan kunci publik seseorang. Setelah memverifikasi identitas pemilik, CA membuat sertifikasi yang merupakan kunci publik pemilik dan data- data lain yang telah ditandatangani secara digital oleh CA. Certificate Authority (CA) bertindak sebagai notaris dengan memverifikasi identitas seseorang dan memberikan sertifikat yang menjamin kunci publik dari individu tertentu. Agen sertifikasi ini menandai sertifikat dengan kunci privatnya sendiri.
Karena itu, individu diverifikasi sebagai pengirim jika kunci publik orang tersebut dapat membuka data. Sertifikat terdiri dari nama subyek, kunci public subyek, nama dari otoritas sertifikat, dan periode dimana sertifikat masih valid. Untuk memverifikasi tanda tangan CA, kunci publiknya harus di sertifikasi silang dengan CA yang lain. Sertifikat ini kemudian dikirim ke repositori, yang menyimpan sertifikat dan Certificate Revocation Lists (CRL) yang menunjukkan sertifikat yang ditarik. SSL (Secure Socket Layer) merupakan protocol keamanan yang menggunakan sertifikat digital. SSL dikembangkan oleh Netscape pada tahun 1994 untuk transaksi client server Internet yang aman. Protokol SSL mengotentikasi server kepada client menggunakan kriptografi kunci publik dan sertifikat digital. Sebagai tambahan, protokol ini juga menyediakan untuk otentikasi client ke server opsional. SSL mendukung penggunaan algoritma kunci publik RSA, algoritma kunci rahasia IDEA, DES dan 3DES, dan fungsi hash MD5. Halaman web menggunakan protocol SSL mulai dengan HTTP, SSL 3.0 dan suksesornya, protokol Transaction Layer Security (TLS) 1.0 adalah standar de fakto, tetapi mereka tidak menyediakan kemampuan end to end dari SET. TLS mengimplementasi kerahasiaan, otentikasi, dan integritas diatas lapisan Transport, dan ada diantara aplikai dan lapisan TCP. Dengan demikian, TLS, dengan SSL dapat digunakan dengan aplikasi seperti Telnet, FTP, HTTP, dan protokol email. Baik SSL dan TLS menggunakan sertifikat untuk verifikasi kunci publik yang berdasar pada standar X.509.

Firewall

Firewall dapat didefinisikan sebagai sebuah komponen atau kumpulan

komponen yang membatasi akses antara sebuah jaringan yang diproteksi dari internet, atau antara kumpulan-kumpulan jaringan lainnya. Firewall dapat berupa hardware dalam bentuk Router atau PC Router, atau software yang menjalankan sistem gateway, atau kombinasi keduanya. Dengan menggunakan firewall maka kita dapat memproteksi paket-paket data yang dikirim ke jaringan internal. Sebuah firewall mempelajari setiap paket data yang dikirim dari atau ke komputer kita dan melihatnya apakah sesuai dengan kriteria yang diberikan. Firewall kemudian akan menyeleksi paket mana yang bisa lewat atau yang harus diblok.



Gambar 8.
Firewall

Tujuan utama Firewall digunakan adalah untuk memastikan sumber-sumber yang tidak dipercayai yang berada di jaringan external memasuki dan menyusup kedalam jaringan internal. Secara umum mengimplementasikan keamanan boleh dikatakan bahwa Firewall sistem jaringan sehingga membatasi hak-hak akses bagi dunia jaringan internal maupun external. Secara umum Firewall berfungsi untuk:

a. Mengatur dan mengontrol lalu lintas jaringan
b. Melakukan autentikasi terhadap akses
c. Melindungi sumber daya dalam jaringan privat
d. Mencatat semua kejadian, dan melaporkan kepada administrator

Network Firewall didesain untuk melindungi jaringan secara keseluruhan dari berbagai serangan. Umumnya dijumpai dalam dua bentuk, yakni sebuah perangkat terdedikasi atau sebagai sebuah perangkat lunak yang diinstalasikan dalam sebuah server. Contoh dari firewall ini adalah Microsoft Internet Security and Acceleration Server (ISA Server), Cisco PIX, Cisco ASA, IPTables dalam sistem operasi GNU/Linux, pf dalam keluarga sistem operasi Unix BSD, serta SunScreen dari Sun Microsystems, Inc. yang dibundel dalam sistem operasi Solaris. Network Firewall secara umum memiliki beberapa fitur utama, yakni apa yang dimiliki oleh personal firewall (packet filter firewall dan stateful firewall),

Circuit Level Gateway, Application Level Gateway, dan juga NAT Firewall. Network Firewall umumnya bersifat transparan (tidak terlihat) dari pengguna dan menggunakan teknologi routing untuk menentukan paket mana yang diizinkan,dan mana paket yang akan ditolak. Firewall bekerja dengan mengamati paket IP (Internet Protocol) yang melewatinya. Berdasarkan konfigurasi dari firewall maka akses dapat diatur berdasarkan IP address, port, dan arah informasi. Detail dari konfigurasi bergantung kepada masing- masing firewall. Firewall pada dasarnya dapat dikategorikan menjadi 2 berdasarkan cara fungsi kerjanya (keduanya dapat dilakukan pada sebuah perangkat computer /device atau dilakukan secara terpisah), yaitu :

1. Fungsi filtering

Firewall bekerja pada level jaringan (network -level firewall) biasa disebut packet filter. Firewall tipe ini biasanya berupa router yang melakukan fungsi packet filtering berdasarkan parameter-parameter tertentu : alamat sumber, protokol, nomor port dan isi. Dari membandingkan informasi yang diperoleh pada paket – paket trafik dengan kebijaksanaan yang ada pada tabel akses, maka tindakan yang diberlakukan adalah :

- Melewatkan paket data ke tujuannya (client atau server)
- Memblok paket data

-

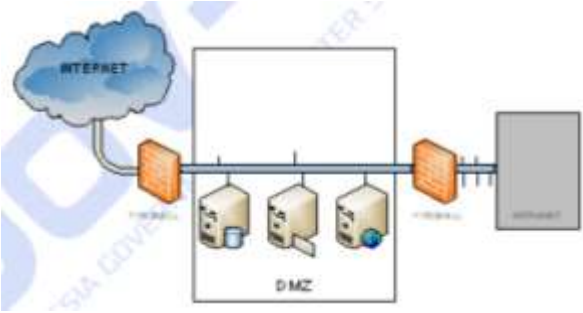
2. Fungsi Proxy

Firewall pada level aplikasi (application level gateway) ini berfungsi sebagai penghubung antara komputer client dengan jaringan luar. Pada koneksinya, paket-paket IP tidak pernah diteruskan secara langsung, namun ditranslasi dan diwakilkan oleh gateway aplikasi tersebut yang berfungsi sebagai saluran dan penterjemah dan menggantikan fun gsi client. Proxy akan merelai semua request dari client kepada server yang sesungguhnya, kemudian merelay balik semua hasil response real server kepada client kembali. Ditengah proses di atas, maka proxy server berkesempatan untuk melakukan pembatasan “relay” berdasarkan tabel akses yang sudah dibuat. Fungsi proxy dapat dilakukan oleh berbagai software tergantung kepada jenis proxy yang dibutuhkan, misalnya web proxy, rlogin proxy, ftp proxy dan seterusnya.

DMZ

DMZ atau DeMilitarized Zone merupakan area bebas dalam jaringan yang dibatasi/ diapit oleh oleh 2 firewall. DMZ digunakan apabila Intranet bisa diakses dari luar secara remote melalui jaringan internet. Komputer-komputer server yang berada pada area DMZ bisa dihubungi dari luar mealaui jaringan internet, misal web server dan e-mail server. Karena bisa dihubungi dari luar maka komputer-komputer ini harus dipersiapkan secara khusus, karena bisa berhubungan secara terbuka dengan pihak luar. Aplikasi yang digunakan pada sesrver-server tersebut harus aman dan dapat dipantau secara terus-menerus. Aturan-aturan yang berlaku pada DMZ adalah sebagai berikut :

- Pihak luar hanya dapat berhubungan dengan server yang berada pada daerah DMZ sesuai dengan kebutuhan yang ada, tidak bisa berhubungan dengan host-host pada internal.
- Host-host pada internal dapat berhubungan dengan web server intranet maupun internet. Pada beberapa implementasi, host-host jaringan internal yang akan berhubungan dengan internet harus dilewatkan melalui proxy, tidak boleh langsung berhubungan dengan internet.



Gambar 9.
Arsitektur DMZ

IDS

IDS atau Intrusion Detection System adalah sebuah aplikasi perangkat lunak atau perangkat keras yang dapat mendeteksi aktifitas yang mencurigakan dalam sebuah sistem atau jaringan. Suatu IDS dapat berupa IDS berbasiskan jaringan atau berbasiskan host. Pada IDS berbasiskan jaringan, IDS akan menerima salinan paket yang ditujukan pada sebuah host untuk kemudian memeriksa paket-paket tersebut. Apabila ternyata ditemukan paket yang berbahaya, maka IDS akan

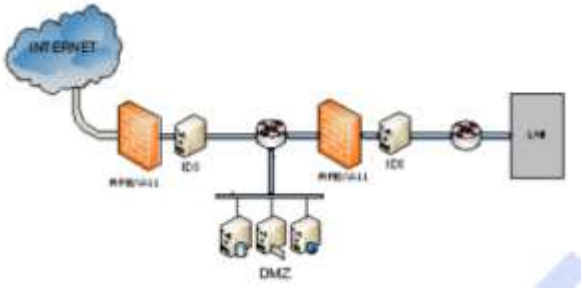
memberikan peringatan pada pengelolah sistem. Karena paket yang diperiksa hanyalah salinan dari paket yang asli, maka sekalipun ditemukan paket yang berbahaya, paket tersebut akan tetap mencapai host yang ditujunya. IDS biasanya bekerja sama dengan IPS (Intrution Prevention System). Suatu IPS bersifat lebih aktif daripada IDS. Bekerja sama dengan firewall, sebuah IPS dapat memberikan keputusan apakah sebuah paket dapat diterima atau tidak oleh sistem. Apabila IPS menemukan bahwa paket yang dikirimkan adalah paket yang berbahaya, maka IPS akan memberitahu firewall sistem untuk menolak paket data tersebut. Dalam membuat keputusan apakah sebuah paket data berbahaya atau tidak, IDS dan IPS dapat mempergunakan metode : Signature-based Intrusion Detection System.
Pada metode ini, telah tersedia daftar signature yang dapat digunakan untuk menilai apakah paket yang dikirimkan berbahaya atau tidak. Sebuah paket data akan dibandingkan dengan daftar yang sudah ada. Metode ini akan melindungi sistem dari jenis-jenis serangan yang sudah diketahui sebelumnya. Oleh karena itu, untuk tetap menjaga keamanan sistem jaringan komputer, data signature yang ada harus tetap ter-update.

Anomaly-based Intrusion Detection System.

Pada metode ini, pengelola jaringan harus melakukan konfigurasi terhadap IDS dan IPS, sehingga IDS dan IPS dapat mengatahui pola paket seperti apa saja yang akan ada pada sebuah sistem jaringan komputer. Sebuah paket anomali adalah paket yang tidak sesuai dengan kebiasaan jaringan komputer tersebut. Apabila IDS dan IPS menemukan ada anomali pada paket yang diterima atau dikirimkan, maka IDS dan IPS akan memberikan peringatan pada pengelola jaringan (IDS) atau akan menolak paket tersebut untuk diteruskan (IPS). Untuk metode ini, pengelola jaringan harus terus-menerus memberi tahu IDS dan IPS bagaimana lalu lintas data yang normal pada sistem jaringan komputer tersebut, untuk menghindari adanya salah penilaian oleh IDS atau IPS. Penggunaan IDS dan IPS pada sistem jaringan komputer dapat mempergunakan sumber daya komputasi yang cukup besar, dan khusus untuk IPS, dengan adanya IPS maka waktu yang dibutuhkan sebuah paket untuk dapat mencapai host tujuannya menjadi semakin lama, tidak cocok untuk aplikasi-aplikasi yang membutuhkan pengiriman data secara real-time. Selain itu IDS dan IPS masih membuka kesempatan untuk terjadinya false-postive dimana sebuah paket yang aman dinyatakan berbahaya dan false-negative dimana paket yang berbahaya dinyatakan

aman. Untuk mengurangi tingkat false-positive dan false-negative, perlu dilakukan pembaharuan secara rutin terhadap sebuah IDS dan IPS.

Dalam implementasinya, IDS adalah sebuah unit host yang terhubung pada sebuah hub/switch dan akan menerima salinan dari paket-paket yang diproses oleh hub/switch tersebut. Sedangkan untuk IPS biasanya diletakkan pada unit yang sama dengan firewall dan akan memproses paket-paket yang lewat melalui firewall tersebut.
Pada IDS berbasiskan host, IDS akan memeriksa aktivitas system call, catatan kegiatan dan perubahan pada sistem berkas pada host tersebut untuk mencari anomali atau keanehan yang menandakan adanya usaha dari pihak luar untuk menyusup kedalam sistem. IDS berbasiskan host akan membantu pengelola system untuk melakukan audit trail terhadap sistem apabila terjadi penyusupan dalam sistem. Salah satu aplikasi perangkat lunak IDS berbasis jaringan yang terkenal adalah snort (snort.org). Snort merupakan aplikasi IDS yang paling populer, gratis, mudah di konfigurasi dan mudah digunakan. Tersedia add-on dan utility khusus snort. Snort melakukan real time traffic analysis dan mengamati event “aneh” yang bias berpotensi usaha penyusupan. Berbasis pada trafik jaringan, Snort mampu mendeteksi lebih dari 1000 potensi kerawanan. Dalam pemakaiannya, snort dapat diaplikasikan pada Demiliterized Zone maupun jaringan internal (LAN). Sehingga setiap ada potensi penyusupan, baik ke server- server publik maupun melalui VPN yang akan mengakses server-server internal atau komputer klien, dapat didetaksi lebih dini



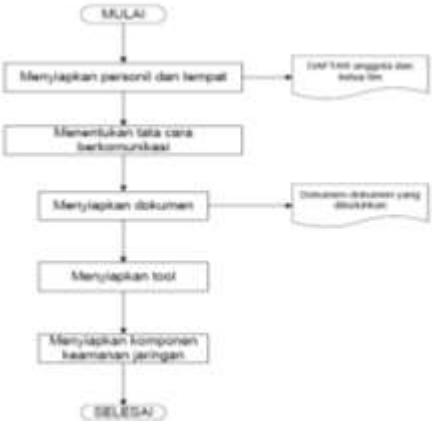
Gambar 10.
Penempatan IDS

Router

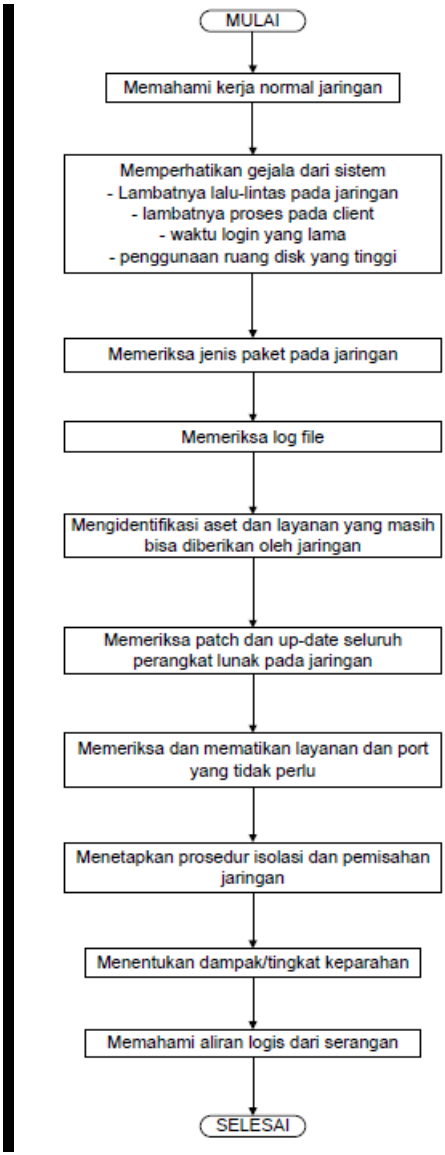
Sementara firewall biasanya membatasi aktivitas jaringan masuk dan keluar berdasarkan kombinasi dari layanan dan alamat IP host, router biasanya dikonfigurasi dengan lebih luas. Biasanya organisasi menggunakan satu atau lebih router dimana jaringan organisasi terhubung ke Internet, router-router ini biasanya dikenal sebagai router perbatasan internet. Router biasanya ditempatkan di depan utama melalui firewall. Router melakukan beberapa pemeriksaan dasar pada aktivitas jaringan, seperti penyaringan ingress dan egress penyaringan, yang mungkin membantu dalam menghentikan beberapa worm berbasis Internet untuk mencapai firewall organisasi. Meskipun firewall juga harus memblokir worm tersebut, setelah router perbatasan internet melakukannya dapat mengambil beberapa beban tanggung jawab firewall .

Selama insiden worm, organisasi mungkin perlu mengkonfigurasi ulang beberapa router perbatasan internet untuk memblokir aktivitas worm yang masuk sehingga firewall tidak menjadi kelebihan beban. Router di jaringan internal dapat dikonfigurasi ulang untuk memblokir aktivitas untuk layanan tertentu agar tidak melewati daerah antara jaringan, hal ini dapat mencegah host yang terinfeksi menyebarkan malware kepada jaringan yang lain.Organisasi harus siap untuk mengubah daftar kontrol akses router (ACL) dengan cepat bila diperlukan untuk membantu dalam menangani infeksi cacing.

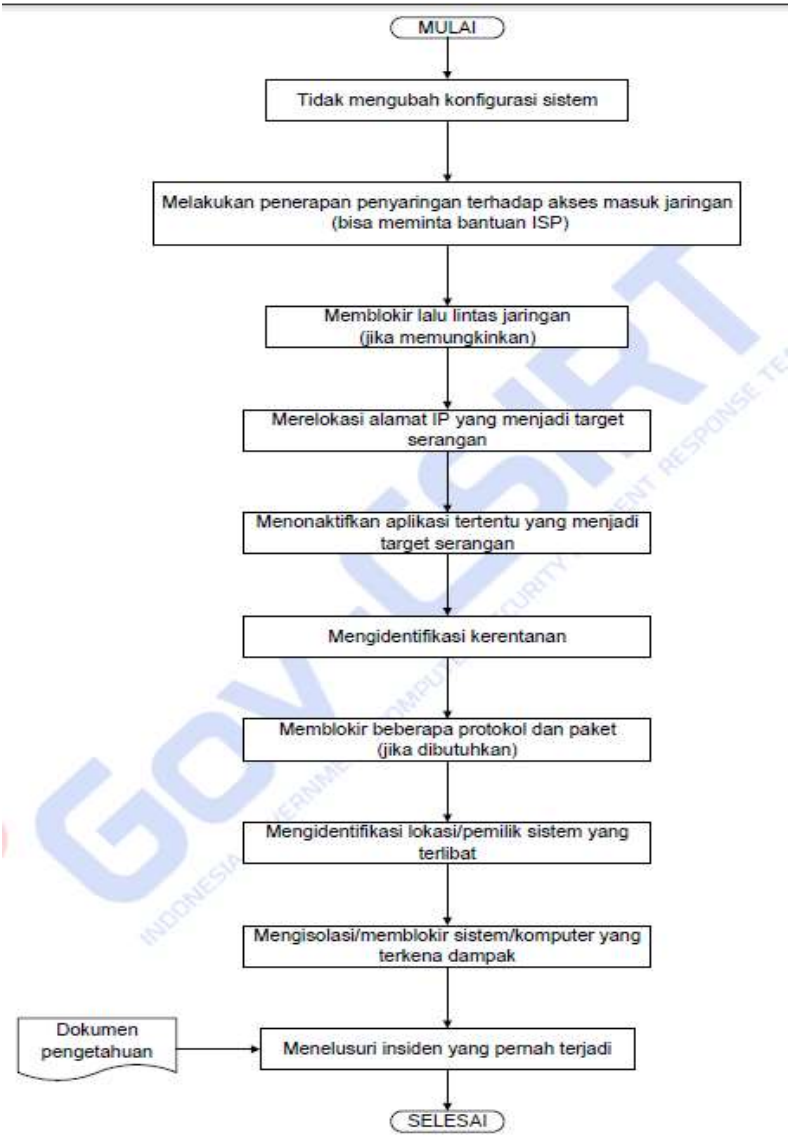
LAMPIRAN B – Diagram Alir



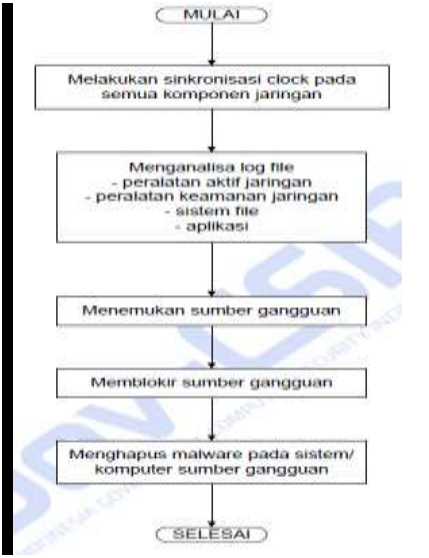
LANGKAH-LANGKAH PADA TAHAP PERSIAPAN



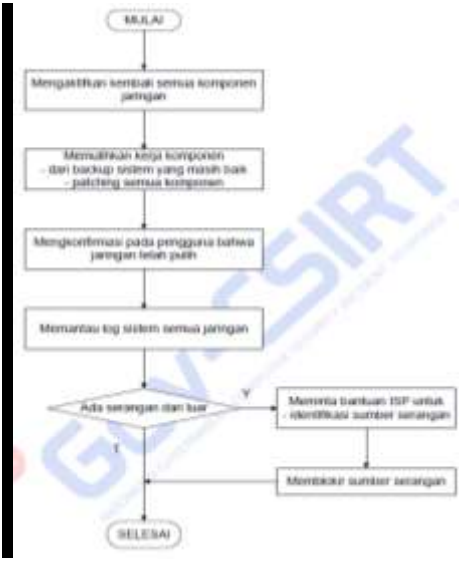
LANGKAH-LANGKAH PADA TAHAP IDENTIFIKASI



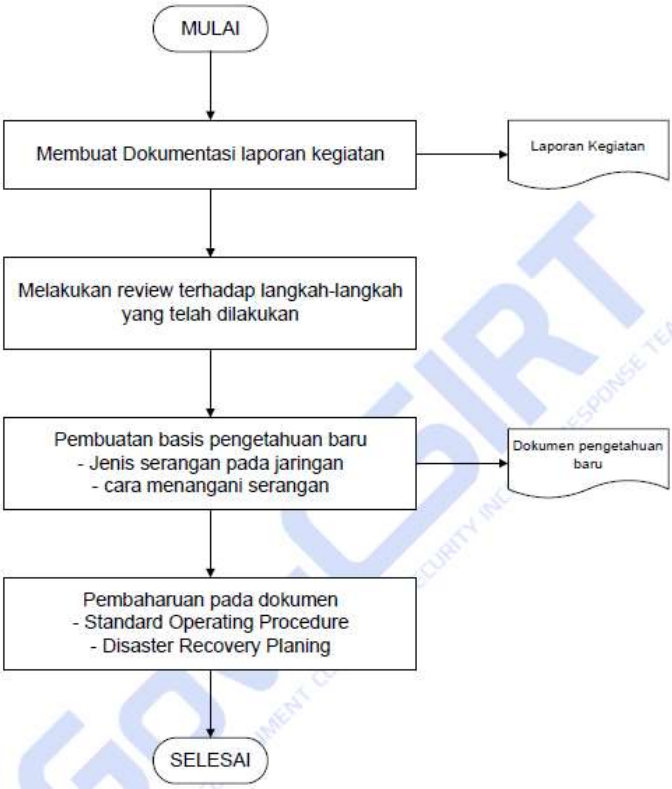
LANGKAH-LANGKAH PADA TAHAP CONTAINMENT



LANGKAH-LANGKAH PADA TAHAP ERADICATION



LANGKAH-LANGKAH PADA TAHAP RECOVERY



LANGKAH-LANGKAH PADA TAHAP TINDAK LANJUT

LAMPIRAN C - Formulir

Formulir laporan penanganan insiden

1. Informasi Pembuat Laporan	
Nama Lengkap	
Jabatan pada tim	
Internal/External	
Nama Institusi (external)	
Nomor Telepon tempat kerja	
Nomor HP	
Alamat E-mail	
Nomor Fax	

Informasi tambahan

2. Jenis insiden : Network

Nomor insiden : .....

- ☐ Akibat malware
- ☐ *DOS*
- ☐ *DDOS*
- ☐ Pemindaian port
- ☐ Akses ilegal (*Packet sniper/capture)*
- ☐ Lainnya .....

Deskripsi singkat dari insiden:

3. Cakupan dari insiden (pilih salah satu)	
☐ Kritis (misal, berpengaruh pada sumber daya informasi yang membahayakan keamanan umum secara luas di luar institusi/lembaga) ☐ Besar (misal, berpengaruh pada seluruh jaringan dan/atau sistem bisnis utama dari nstitusi/lembaga) ☐ Sedang (misal, hanya berpengaruh pada infrastruktur jaringan, server, atau akun admin pada institusi/lembaga) ☐ Kecil (misal, hanya berpengaruh pada komputer atau akun pengguna pada institusi/lembaga)	
Perkiraan jumlah sistem yang terkena dampak:	
Perkiraan jumlah pengguna yang terkena dampak:	
Pihak ketiga yang terkena dampak: (misal: vendor, kontraktor, partner)	
Informasi tambahan dari cakupan insiden:	

4. Dampak dari insiden	
☐ Berhenti/hilangnya layanan ☐ Berhenti/hilangnya produktifitas ☐ Hilangnya reputasi ☐ Berkurang/hilangnya pendapatan	☐ Penjalaran ke jaringan lain ☐ Pengungkapan tidak sah dari data/informasi ☐ Pengubahan tidak sah dari data/informasi ☐ Lainnya, ...
Informasi lain dari dampak insiden	

5. Sensitivitas dari data yang terkena insiden	
☐ Data/info rahasia/sensitiv ☐ Data/info Non-sensitive ☐ Data/info yang disediakan untuk publik ☐ Data/info keuangan	☐ Informasi Identitas Pribadi Personil ☐ Data/info tentang HAKI/*copyrighted* ☐ Data/info tentang *critical infrastructure/key resources* ☐ Lainnya, ...
Data dienkripsi ? Ya ____ tidak ____	
Besarnya data/informasi yang terkena insiden: (ukuran file, jumlah record)	
Informasi tambahan:	

6. Sistem yang terkena insiden	
Sumber serangan *(alamat IP, port)*:	
Tujuan serangan *(alamat IP, port)*:	
Alamat IP dari sistem:	
Nama Domain dari sistem:	
Fungsi dari sistem: *(web server, domain controller)*	
Sistem Operasi dari sistem: *(version, service pack, configuration)*	
Level Patching dari sistem: *(latest patches loaded, hotfixes)*	
Perangkat lunak security pada sistem: *(anti-virus, anti-spyware, firewall, versions, date of latest definitions)*	
Lokasi fisik dari sistem: *(propinsi, kota, gedung,ruang,meja/rak/lemari)*	
Informasi tambahan dari sistem:	

7. Pengguna yang terkena dampak	
Nama dan jenis pekerjaan pengguna:	
Level hak akses dari pengguna: *(regular user, domain administrator, root)*	
Informasi tambahan pengguna:	

8. Timeline dari insiden	
Tanggal dan waktu kejadian pertama kali terdeteksi, ditemukan, atau diberitahu tentang insiden itu:	
Tanggal dan waktu saat kejadian yang sebenarnya terjadi: (perkiraan, jika tanggal dan waktu yang tepat tidak diketahui):	
Tanggal dan waktu ketika insiden itu ditangani atau ketika semua sistem/fungsi telah dipulihkan(menggunakan tanggal dan waktu terakhir):	
Tenggang waktu antara penemuan dan kejadian : Tenggang waktu antara penemuan dan pemulihan :	
Keterangan tambahan:	

9. Pemulihan dari insiden	
Tindakan yang dilakukan untuk mengidentifikasi sumber daya yang terkena dampak:	
Tindakan yang dilakukan untuk memulihkan insiden:	
Rencana tindakan untuk mencegah berulangnya insiden:	
Informasi tambahan pemulihan insiden:	

LAMPIRAN D – Formulir Setiap Tahap

Form untuk tahap Persiapan

Form untuk tahap Persiapan

Hari/tanggal:	
Waktu:	
Nama anggota tim pengisi form: Tanda tangan:	

Persiapan	
Nama anggota tim	Ketua : ..... Anggota : 1. ..... 2. ..... 3. .....
Metode komunikasi	☐ Handphone ☐ Email ☐ Tlp. kantor
Dokumen yang dibutuhkan	1. ..... 2. ..... 3. ..... 4. .....
Tool/alat yang digunakan	1. ..... 2. ..... 3. ..... 4. .....
Komponen keamanan jaringan	1. ..... 2. ..... 3. ..... 4. .....

Form untuk tahap *Identifikasi*

Hari/tanggal:	
Waktu:	
Nama anggota tim pengisi form: Tanda tangan:	

Penjelasan secara singkat tentang insiden network yang terjadi	
Penjelasan secara singkat dampak dari insiden network	
Berapa banyak sistem informasi/layanan yang terdapat pada sistem jaringan yang terpengaruh oleh insiden jaringan	
Penjelasan secara singkat kapan dan dimana insiden jaringan pertama kali diketahui	

Form untuk tahap *Containment*

Hari/tanggal:	
Waktu:	
Nama anggota tim pengisi form: Tanda tangan:	

Penghentian akses kepada system, layanan, dan data	
Penjelasan tentang akses, sistem, dan layanan yang telah dinonaktifkan karena adanya insiden	
Pencatatan waktu saat semua akses, sistem, dan layanan dinonaktifkan	

Informasi Sistem Back up	
Apakah back up sistem berhasil dilakukan ?	☐ Ya ☐ Tidak, jika tidak, apakah penyebabnya ?
Nama personil yang melakukan back up	
Waktu proses back up dimulai	
Waktu prosees back up selesai	
Apakah media back up dilindungi dan disegel?	☐ Ya ☐ tidak, Jika tidak, apakah penyebabnya ?

Form untuk tahap *Eradication*

Hari/tanggal:	
waktu:	
Nama anggota tim pengisi form: Tanda tangan:	

Nama Sistem	
Nama semua personil yang melakukan proses forensik terhadap sistem yang mengalami insiden	
Apakah kerentanan yang menyebabkan insiden keamanan dapat teridentifikasi?	☐ Ya ☐ Tidak, jika ya, deskripsikan secara detail
Jelaskan prosedur validasi yang digunakan untuk memastikan bahwa – kerentanan telah dikurangi – penyebab gangguan telah dihilangkan	

Form untuk tahap *Follow Up*

Hari/tanggal:	
waktu:	
Nama personil pengisi form: Tanda tangan:	

Jelaskan secara singkat tentang insiden keamanan yang terjadi dan tindakan apa yang telah diambil	
Berapa banyak waktu yang dihabiskan untuk menangani insiden tersebut ?	
Adakah biaya (langsung dan tidak langsung) dari insiden itu ?	
Apa nama organisasi/institusi yang telah mambantu dan dapat melakukannya dengan baik dalam menangani dan mengelolah insiden tersebut ?	
Kesulitan apa yang dihadapi dalam menangani dan mengelolah insiden tersebut ?	
Apakah ada persiapan yang memadai dalam nenangani kejadian tersebut ?	
Apakah deteksi insiden terjadi segera ? Jika tidak, mengapa ?	
Alat tambahan apa yang bisa digunakan untuk membantu dalam merespon dan mengelolah insiden keamanan ?	
Apakah komunikasi antara anggota tim cukup memadai ? Jika tidak, apa yang bisa diperbaiki ?	
Apakah komunikasi dengan organisasi-organisasi luar yang telah membantu cukup memadai ? Jika tidak, apa yang bisa diperbaiki ?	
Apakah prosedur perbaikan telah memadai untuk mencegah terjadinya insiden yang sama pada masa depan ?	