Penanganan dan Pencegahan Insiden pada Serangan DoS di Jaringan Komputer Sesuai Rekomendasi NIST 800-61

EL6115 Secure Operation and Incident Response

Syaiful Andy 13212050

Sekolah Teknik Elektro dan Informatika

Institut Teknologi Bandung, Indonesia

Abstrak

Operasi yang aman sudah menjadi kewajiban bagi perusahaan dan organisasi yang memanfaatkan teknologi informasi dalam proses bisnisnya. Operasi keamanan ini ditujukan agar CIA (Confidentiality, Integrity, dan Authentication) dari perusahaan terjaga. Meskipun operasi keamanan sudah dijalankan oleh perusahaan, terkadang masih mungkin terjadi adanya insiden keamanan di perusahaan karena berbagai sebab. Salah satu insiden klasik yang cukup sering terjadi adalah adanya serangan denial of service (DoS). Dalam makalah ini akan dibahas bagaimana cara penanggulanan insiden DoS pada jaringan yang sesuai dengan standar NIST 800-61 [1]. Pembahasan dimulai dari tahap persiapan sebelum terjadinya insiden, kemudian pendeteksian dan analisis, dan terakhir tahap recovery sistem. Selain itu, akan dibahas juga mengenai usaha-usaha yang harus dilakukan oleh petugas jaringan untuk mencegah adanya serangan DoS.

Kata kunci — *penanganan insiden, DoS, NIST*

1. Pendahuluan

Saat ini penggunaan teknologi informasi di berbagai bidang dalam kehidupan sehari-hari merupakan sesuatu yang sudah biasa. Hal itu disebabkan karena

semakin majunya teknologi, sehingga teknologi informasi dapat membantu mempermudah kegiatan sehari-hari. Disisi lain, jumlah kejahatan komputer (computer crime), terutama yang berhubungan dengan sistem informasi jumlahnya terus meningkat [2]. Hal tersebut tentunya membawa kekhawatiran tersendiri bagi pengguna teknologi informasi. Oleh karena itu, keamanan dari teknologi informasi menjadi hal yang sangat penting untuk di perhatikan.

Garfinkel dalam bukunya mengemukakan bahwa keamanan komputer mencakup empat aspek, yaitu *privacy, integrity, authentication,* dan *availability* [3]. Sedangkan menurut buku yang dikeluarkan oleh ISACA [4], objek dari keamann informasi terdiri dari tiga komponen, yaitu *confidentiality, integrity,* dan *availability*. *Confidentiality* berarti melindungi ingormasi dari akses yang tidak diizinkan, *integrity* berarti melindungi dari perubahan data yang tidak diizinkan, sedangkan *availability* berarti melindungi informasi agar tetap dapat diakses. Ketiga komponen tersebut terkait erat dengan perlindungan informasi. Adanya insiden berupa serangan terhadap teknologi informasi tentunya dapat mengganggu komponen dari keamanan informasi tersebut. Berikut disajikan data statistik terkait laporan insiden tahun 2015 yang dikeluarkan oleh ID CERT [6] ditunjukkan pada tabel (1). Terlebih lagi, jenis serangan yang begitu banyak

No Rating	*Complaint Category 2015*	*Rating (%)*
1	*Intellectual Property Right (IPR) /HAKI*	*41.24*
2	*Spam*	*30.32*
3	*Spam complaint*	*9.99*
4	*Network Incident (Deface, DdoS attack, etc)*	*7.41*
5	*Spoofing/Phishing*	*3.72*
6	*Malware*	*2.76*

Table 1: Statistik Laporan Insiden yang diterima ID CERT

macamnya tentunya membuat pengelola informasi kesulitan. Oleh karena itu, saat ini biasanya ada tim khusus yang sering disebut sebagai *computer security incident response teams* (CSIRTs) yang bertugas menangani insiden. Selain itu, penting juga dilakukan upaya-upaya pencegahan agar kemungkinan terjadinya insiden dapat diperkecil, walaupun tidak semua insiden dapat dicegah[5].

Dalam makalah ini, pembahasan akan dikhususkan mengenai salah satu insiden yang berpengaruh terhadap *availability* dari sistem informasi. Insiden yang dimaksud adalah serangan *denial of service* (DoS) yang dapat mengakibatkan ketersediaan dari informasi terganggu. Makalah ini akan membahas teknik-teknik yang dilakukan dalam menangani insiden DoS dimulai dari tahap

persiapan sebelum terjadinya insiden, kemudian pendeteksian dan analisis, dan terakhir tahap recovery sistem. Pembahasan mengenai penanganan insiden DoS dalam makalah ini mengikuti rekomendasi yang diberikan oleh *National Institute of Standards and Technology* (NIST) 800-61. Selain itu dibahas juga usaha-usaha yang dapat dilakukan agar insiden DoS dapat dicegah sehingga kemungkinan terganggunya *availability* dari sistem informasi dapat diminimalisir.

2. Tinjauan Pustaka

Pada bagian ke dua ini akan dipaparkan tinjauan pustaka mengenai penelitian yang berhubungan dengan topik makalah antara lain: model proses umum respon insiden dan forensik komputer, model umum investigasi forensik komputer, dan metodologi investigasi bertahap untuk menelusuri penggunaan komputer.

2.1. Penanganan Insiden Secara Umum

Penanganan insiden yang diterapkan oleh suatu organisasi memiliki beberapa fase. Pada fase awal persiapan penanganan insiden, perlu adanya pembentukan tim, pelatihan, dan mencari perangkat dan sumber daya yang dibutuhkan untuk penanganan insiden. Selama masa persiapan ini, organisasi yang bersangkutan harus berusaha agar jumlah insiden yang mungkin akan terjadi dapat dibatasi dengan cara mengimplementasikan beberapa aturan kontrol sesuai dengan hasil *risk assessment*. Walaupun aturan kontrol tadi sudah ditetapkan, masih memungkinkan adanya insiden yang dapat terjadi. Oleh karena itu, perlu adanya fase pendeteksian dan analisis dari bobolnya keamanan informasi milik organisasi ketika terjadi insiden terjadi. Setelah insiden terdeteksi, fase berikutnya adalah fase penanganan insiden dan pemulihan sistem. Organisasi harus segera menangani insiden yang terjadi dengan cepat dan segera memulihkan kondisi sistem agar sistem informasi organisasi tersebut kembali berjalan dengan normal. Selama fase ini, terkadang perlu memperhatikan fase sebelumnya yaitu pendeteksian dan analisis disebabkan masih ada kemungkinan insiden lainya terjadi lagi, misalnya saja satu komputer di organisasi tersebut yang terkena virus, insiden ini terdeteksi oleh tim penanganan insiden dan segera ditangani, nmun bisa jadi, selama masa penanganan tersebut komputer lainya dalam organisasi tersebut terkena virus. Setelah insiden benar-benar telah selesai ditangani, tim penanganan insiden harus membuat laporan yang berisi detail

dari penyebab, biaya yang dikeluarkan, dan langkah-langkah penanganan insiden tersebut agar insiden tersebut dapat dicegah dikemudian hari [1]. Gambar (1) mengilustrasikan dari fase penanganan insiden.

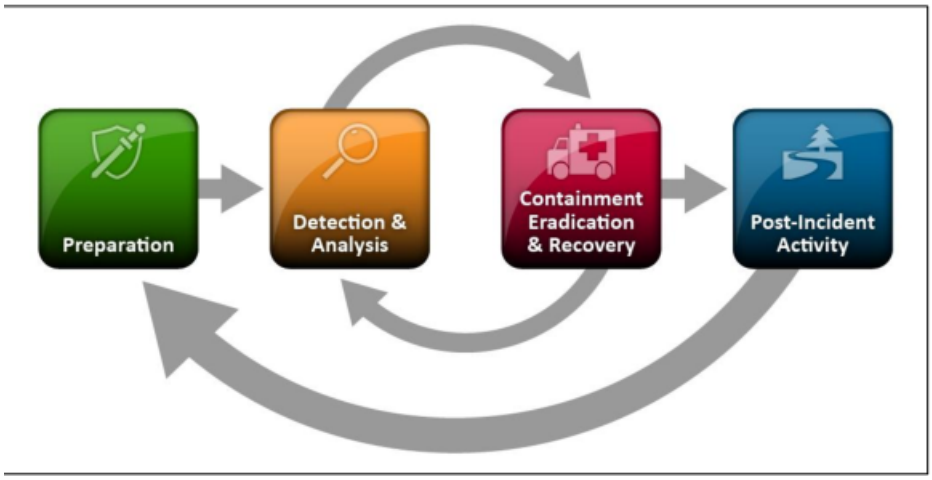

Figure 1: Incident Response Life Cycle

2.1.1. Tahap Persiapan

Penanganan insiden biasanya difokuskan pada tahap persiapan. Hal tersebut disebabkan karena pada tahap itu, organisasi tidak hanya mempersiapkan kemampuan dalam menangani insiden yang mungkin terjadi, namun juga kemampuan dari organisasi untuk mencegah suatu insiden dapat terjadi dengan membuat sistem, jaringan, dan aplikasi yang digunakan dalam organisasi tersebut cukup aman. Tahap persiapan secara umum terbagi menjadi dua, yaitu persiapan penanganan insiden dan pencegahan insiden. Yang perlu dipersiapkan dalam penanganan insiden adalah perangkat dan sumber daya. Organisasi harus mempersiapkan perangkat komunikasi dan fasilitas untuk melakukan penanganan insiden seperti siapa yang harus dikontak, mekanisme pelaporan insiden, perangkat lunak dan perangkat keras yang diperlukan untuk analisis insiden, backup data untuk pemulihan sistem, dan yang lainya. Sedangkan pencegahan insiden yang dilakukan oleh tim penanganan insiden dapat dilakukan dengan misalnya melakukan *risk assessments* secara periodik untuk mengetahui bahaya yang dapat menyerang ke sistem, memperkuat keamanan komputer yang ada di organisasi, meningkatkan keamanan jaringan organisasi, mencegah malware, dan pelatihan pada orang-orang dalam organisasi tentang kepedulian terhadap

keamanan informasi.

2.1.2. Tahap Deteksi dan Analisis

Insiden dapat terjadi dengan berbagai cara, sehingga tidak ada instruksi tiap langkah yang pasti untuk mendeteksi dan menangani setiap insiden. Namun, tim penanganan insiden di organisasi harus mempersiapkan diri untuk menghadapi insiden yang kemungkinan besar serangan insiden itu berasal. Misalkan, serangan dari media eksternal biasanya berupa virus, *malicious code*, dan lainya. Serangan pada aplikasi web, misalnya *cross site scripting, SQL injection*, dan yang lainya. Serangan terhadap ketersediaan sistem misalnya serangan *distributed* DOS, *brute force*, dan lainya. Untuk tiap serangan yang sudah umum terjadi tersebut harus didefinisikan prosedur penanganan yang dapat diterapkanya.

Kesulitan yang sering dialami oleh kebanyakan tim penanganan insiden dalam organisasi adalah mendeteksi kemungkinan insiden, menentukan apakah insiden benar-benar terjadi, dan bila terjadi, jenis dan dampak dari insiden tersebut harus jelas. Dalam melaksanakan fungsi deteksi insiden, terkadang digunakan indikator-indikator yang berasal dari *Intrusion Detection and Prevention System* (IDPS), *Security Information and Event Management* (SIEM), *antivirus, antispam*, perangkat lunak pendeteksi integritas data, jasa monitoring dari pihak ke tiga, log dari sistem operasi, servis, aplikasi, perangkat jaringan yang beroperasi, informasi dari pihak lain terkait kerentanan terkini dari sistem yang digunakan, dan laporan dari orang dalam dan luar organisasi.

Selanjutnya perlu juga dilakukan analisis lanjutan disebabkan informasi yang didapatkan dari indikator tidak semuanya tepat. Analisis diperlukan agar bisa dipastikan apakah insiden terjadi ataukah tidak. Beberapa cara yang dapat dilakukan untuk melakukan analisis diantaranya adalah dengan melakukan *profiling* (mengukur karakteristik dari aktivitas yang dilakukan) dari sistem dan jaringan, memahami tingkah laku sistem yang normal, membuat kebijakan lamanya penyimpanan log, mengaitkan suatu log dengan log lainya (misal log dari aplikasi yang mengamati user dengan log firewall yang mengamati IP yang mengakses), menjaga agar tiap perangkat di organisasi memiliki waktu yang tersinkronkan agar data di log dapat dianalisis dengan baik, melakukan filter data yang dianggap mencurigakan, dan lainya. Hasil yang didapatkan dari kegiatan pendeteksian dan analisis harus didokumentasikan misalnya dengan membuat logbook agar pekerjaan dapat dilakukan dengan efisien, sistematis, dan dapat dijadikan barang bukti bila terjadi pelanggaran hukum.

Pada tahap deteksi dan analisis ini, bila insiden ditemukan lebih dari satu, maka perlu dibuat skala prioritas dari insiden. Insiden yang memiliki prioritas lebih tinggi yang akan ditangani lebih dahulu. Beberapa pertimbangan dalam memberikan skala prioritas adalah sebagai berikut.

1. Dampak fungsional dari insiden, seberapa besar dampak yang ditimbulkan oleh insiden terhadap fungsionalitas dari keberjalanan fungsi bisnis organisasi saat itu dan di masa depan bila insiden tersebut tidak segera ditangani.
2. Dampak Informasi dari insiden, seberapa pengaruhnya insiden ini terhadap *confidentiality, integrity,* dan *availability* dari informasi yang ada di organisasi.
3. Kemampuan pemulihan dari insiden, seberapa besar insiden dan sumber daya apa saja yang terkena dampak dari insiden sehingga orang yang menagani insiden dapat memperkirakan waktu dan sumber daya yang dibutuhkan untuk menangani insiden tersebut. Beberapa insiden tidak dapat dipulihkan (misalnya saja kerahasiaan data yang bocor), namun ada usaha yang dapat dilakukan agar insiden serupa tidak terjadi kembali.

2.1.3. Tahap Penanganan dan Pemulihan

Penanganan insiden dilakukan dengan menahan agar insiden tidak meluas, dan pembasmian insiden. Pada penahanan agar insiden tidak meluas diperlukan strategi yang biasanya di bentuk dalam prosedur penanganan insiden. Selain itu, pencarian bukti dalam insiden kadang diperlukan untuk menyelesaikan insiden. Log yang ada harus disimpan dengan baik sebagai bukti selain itu perlu dijaga juga mengenai informasi identitas (IP komputer, MAC, dan lainya), waktu dan tanggal kejadian, orang-orang yang terlibat dalam insiden, lokasi tempat penyimpanan barang bukti. Pencarian pelaku penyerangan pun kadang diperlukan dengan berbagai sebab meskipun terkadang memakan waktu dan sia-sia, karena yang lebih penting bagi organisasi adalah keberjalanan dari bisnis yang dilakukan.

Pembasmian insiden mungkin diperlukan untuk menghilangkan komponen dari insiden, misalnya membersihkan malware, menghapus akun yang bobol, identifikasi dan mitigasi semua kerentanan yang dibobol. Pada masa pembasmian ini, penting untuk melakukan identifikasi pada seluruh komputer yang terkena dampak insiden di organisasi agar semuanya dapat diperbaiki.Selanjutnya, adalah pemulihan sistem. Administrator mengembalikan sistem agar dapat

menjalankan fungsi operasi yang normal, dan juga menutup kerentanan untuk mencegah insiden yang sebelumnya terulang kembali.

2.1.4. Tahap Pasca Insiden

Salah satu bagian terpenting dari tahap ini yang sering diabaikan adalah pembelajaran apa yang dapat diambil dari insiden sebelumnya dan peningkatan yang harus diterapkan. Hal tersebut diperlukan untuk meningkatkan pengukuran keamanan informasi organisasi dan proses penanganan insiden itu sendiri. Tahap ini biasanya dilakukan dengan mengadakan rapat dengan seluruh pihak yang terlibat setelah insiden berakhir.

2.2. Serangan Denial of Service

Denial of Service (DoS) merupakan aksi yang mencegah atau mengganggu pengguna yang berhak dari mengakses jaringan, sistem, atau aplikasi dengan cara menghabiskan sumber daya seperti *central processing units (CPUs), memory, bandwidth,* dan penggunaan *disk*. Beberapa insiden serangan DoS yang terjadi misalnya pada beberapa *website* yang terkenal sehingga *website* tersebut tidak dapat diakses oleh pengguna, penggunaan seluruh *bandwidth* di jaringan dengan cara memberikan trafik yang sangat besar, pengiriman paket TCP/IP yang "rusak" ke server, sehingga server menjadi *crash*, membuat banyak request ke server yang memakan *resource* dari prosesor yang tinggi, membuat banyak login simultan ke server sehingga pengguna lain yang ingin mengakses tidak dapat login, dan mengkonsumsi banyak ruang pada *disk* di server dengan membuat banyak file yang berukuran besar.

Empat tipe dari serangan DoS yaitu :

1. Serangan reflektor merupakan serangan dari sebuah komputer yang mengirimkan banyak *request* ke *service* pada komputer perantara (berperan sebagai reflektor) dengan alamat pengirim yang telah dipalsukan dengan alamat yang akan diserang. Dengan begitu, respon dari komputer perantara tersebut akan dikirimkan ke alamat pengirim yang telah dipalsukan bukan pengirim yang sesungguhnya. Pemalsuan sumber juga digunakan oleh penyerang untuk menyembunyikan sumber serangan. Pada serangan DoS jenis ini, komputer yang terkena dampaknya yaitu komputer yang alamatnya dipalsukan, komputer perantara, atau keduanya. Ilustrasi dari serangan ini tampak pada gambar (2).
2. Serangan Penguatan merupakan serangan yang mirip dengan serangan reflektor yaitu penyerang mengirimkan *request* dengan alamat palsu (alamat

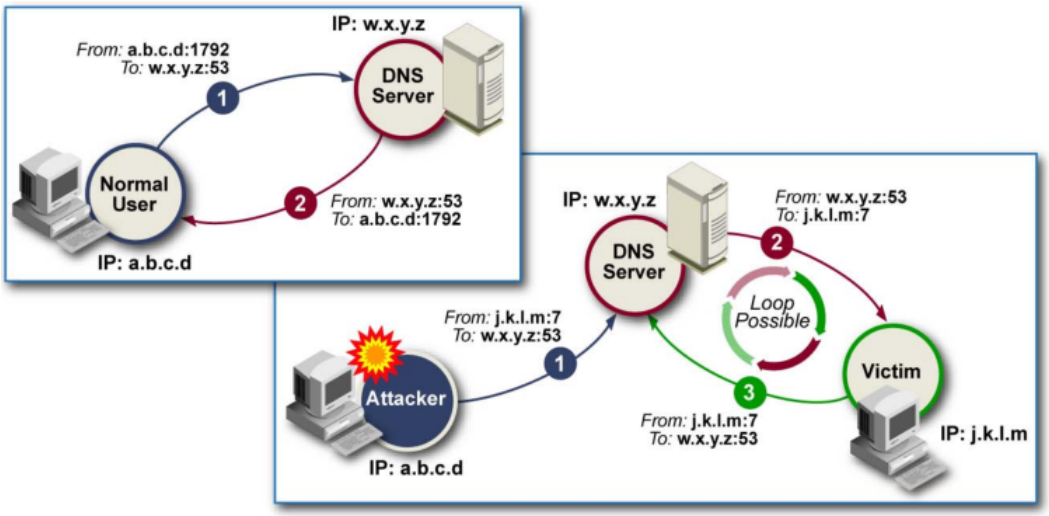

Figure 2: Serangan Reflektor

yang akan diserang). Bedanya adalah pada serangan ini, komputer perantara yang digunakan tidak hanya satu, namun tujuanya adalah menggunakan seluruh jaringan pada *host* perantara. Gambar (3) mengilustrasikan serangan penguatan.

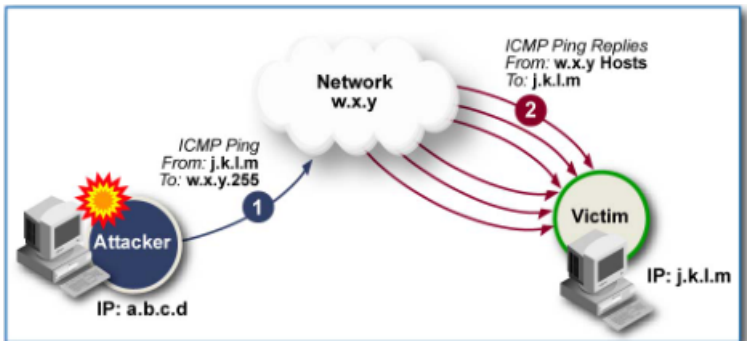

Figure 3: Serangan Penguatan

3. Serangan DoS terdistribusi (DDoS), merupakan serangan DoS yang mengkoordinasikan serangan dari banyak komputer sekaligus. Bila komputer yang digunakan cukup banyak, jumlah trafik jaringan yang dihasilkan bisa saja tidak hanya menghabiskan resource pada *host* yang sedang diserang, namun keseluruhan jaringan pada organisasi tersebut. Gambar (4) mengilus-

trasikan serangan DDoS.

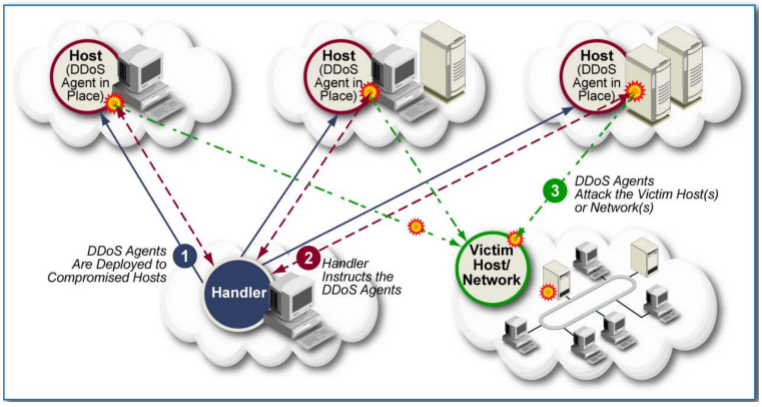

Figure 4: Serangan DDoS

4. Serangan *Synfloods*, merupakan serangan yang disebabkan oleh penyerang yang menginisiasi banyak koneksi TCP dalam jangka waktu yang pendek dengan mengirimkan paket SYN saja sehingga tidak cukup melakukan proses TCP *three-way handshakes* yang dibutuhkan untuk membentuk koneksi yang seharusnya. Gambar (5) mengilustrasikan serangan DoS jenis *Synfloods*.

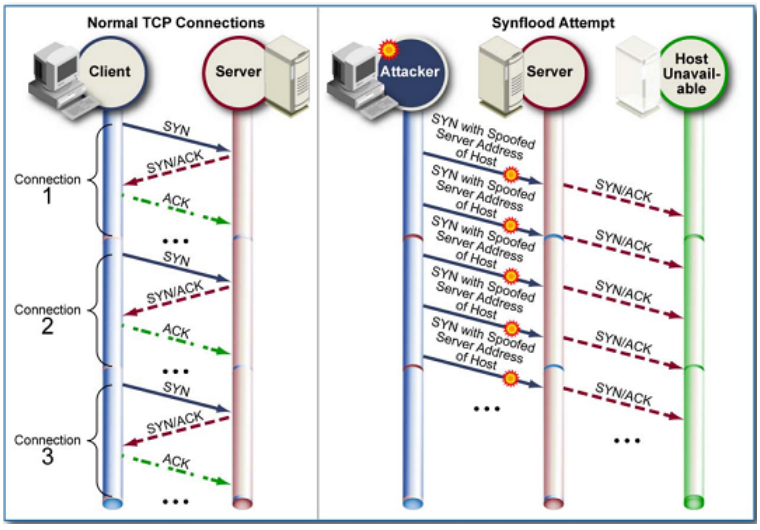

Figure 5: Serangan Synfloods

3. Pembahasan

Pada bagian ini, akan dibahas mengenai penanganan dan pencegahan insiden pada serangan DoS berdasarkan rekomendasi NIST 800-61[5].

3.1. Tahap persiapan

Persiapan yang harus dilakukan untuk serangan DoS selain persiapan yang dilakukan pada bab 2.1.1 sebelumnya, perlu juga melakukan persiapan berikut.

1. Bicarakan dengan penyedia jasa ISP yang digunakan oleh organisasi. Tanyakan bagaimana cara mereka dalam menangani serangan DoS misalnya dengan membatasi trafik di jaringan, menyediakan log terkait trafik DoS, dan melakukan penelusuran darimana sumber serangan berasal.
2. Pertimbangkan kemungkinan investigasi yang membutuhkan koordinasi dari banyak pihak bila serangan DoS yang terjadi meluas ke organisasi lain.
3. Pasang dan konfigurasi perangkat IDS untuk pendeteksian trafik serangan DoS.
4. Buat monitoring penggunaan sumber daya dari *bandwidth* jaringan maupun host dalam organisasi, buat log maupun *alert* bila ada perubahan yang besar dari penggunaan sumber daya yang umum.
5. Analisis dengan bantuan *websites* yang menyediakan statistik dari latensi antara beberapa ISP dan antara beberapa lokasi fisik sebagai salah satu cara monitoring kesehatan internet. Ketika serangan DoS terjadi, orang yang menangani insiden tersebt dapat menggunakan *websites* tersebut untuk menentukan apakah serangan yang mirip mengenai organisasi yang lain.
6. Temui administrator infrastruktur jaringan organisasi untuk mendiskusikan mengenai analisis dan penanganan yang harus dilakukan ketika serangan DoS terjadi. Misalkan dengan menyediakan log yang lebih banyak ketika adanya indikasi serangan DoS. Selain itu, administrator juga berperan dalam menjaga bukti-bukti yang tersimpan dan untuk meminta salinan log untuk dianalisis.
7. Buat salinan lokal dari informasi yang ada pada komputer yang berperan dalam penanganan insiden DoS bila internet internal organisasi mati selama insiden. Hal ini diperlukan untuk mempermudah analisis bila jaringan internet organisasi sedang mati.

Selain persiapan dalam menghadapi insiden diatas, perlu juga diterapkan pencegahan yang dapat dilakukan oleh organisasi untuk mencegah serangan DoS dapat terjadi. Pencegahan secara umum telah dibahas pada bab 2.1.1, pencegahan lainya yang dapat dilakukan oleh tim penanganan insiden adalah sebagai berikut.

1. Konfigurasi perangkat jaringan yang berada antara organisasi dan luar organisasi (*perimeter*) agar menolak semua trafik yang masuk dan keluar bila tidak ada kejelasan izin yang telah ditentukan oleh organisasi, seperti.
   (a) Menutup penggunaan *service port* yang tidak boleh digunakan oleh yang tidak berwenang dan biasanya digunakan untuk serangan DoS seperti *echo* (port 7) dan *chargen* (port 19) .
   (b) Lakukan filtering paket yang masuk dan keluar untuk memblokir paket yang berisi paket tipuan (*spoofed packets*).
   (c) Blokir trafik dari range IP yang belum di *assign* (dikenal dengan list *bogon*). Hal ini disebabkan biasanya perangkat lunak penyerang menipu alamat IP dengan menggunakan alamat IP yang belum di *assign* untuk penggunaan internet.
   (d) Tuliskan *rules* pada *firewall* dan *access control* pada *router* agar memblokir trafik dengan baik. Konfigurasi *rules* pada *firewall* untuk mencegah serangan reflektor, karena kebanyakan serangan reflektor dapat dicegah dengan *rules* yang ada pada firewall dengan menolak semua kombinasi mencurigakan dari port sumber dan port yang dituju.
   (e) Konfigurasi router di area perbatasan antara jaringan internal dan eksternal agar tidak mem*forward* paket yang bersumber dari *broadcast*.
   (f) Batasi jumlah trafik paket ICMP yang masuk dan keluar jaringan agar hanya dalam tipe dan kode tertentu.
   (g) Blokir koneksi ke port IRC, layanan *peer to peer* mapun *instant messaging* bila layanan tersebut tidak diperbolehkan organisasi.
2. Implementasikan batasan trafik yang boleh digunakan oleh protokol tertentu seperti ICMP, sehinga trafik untuk protokol tersebut hanya beberapa persen dari total bandwidth yang ada di organisasi. Pembatasan tersebut dapat dilakukan oleh perangkat jaringan yang berada di perbatasan maupun oleh ISP.

3. Pada *host* yang dapat diakses oleh internet, matikan semua layanan (port) yang tidak dibutuhkan, dan batasi penggunaan layanan yang mungkin sebagai objek serangan DoS.
4. Pasang perangkat lunak pencegah DoS. Perangkat lunak tersebut dapat mempelajari pola penggunaan trafik jaringan, mendeteksi bila adanya perubahan signifikan penggunaan trafik, dan juga memblokir trafik yang mencurigakan. Walaupun deteksi dari perangkat lunak ini terkadang salah sehingga dapat memblokir trafik yang seharunya diperbolehkan atau membiarkan trafik yang sebenarnya adalah serangan DoS. Oleh karena itu, peran dari pengawas jaringan masih diperlukan.
5. Implementasikan *redundancy* pada fungsi-fungsi yang sangat penting bagi organisasi, misalnya penggunaan layanan ISP yang berbeda, *firewall* yang digunakan, maupun *web server*.
6. Pastikan jaringan dan sistem tidak berjalan pada kapasitas yang hampir maksimal. Hal ini karena bila penggunaan normal sudah mendekati kapasitas maksimal, maka serangan DoS yang kecil dapat menghabiskan sisa dari sumber daya yang tersedia.

3.2. Tahap Deteksi dan Analisis

Serangan DoS dapat dideteksi melalui beberapa tanda dan indikasi. Pada tabel (2) menunjukkan tanda dari serangan DoS dan respon rekomendasi yang seharusnya dilakukan untuk mencegah insiden ini berlanjut.

Tanda	Respon
Biasanya serangan DoS diawali dengan aktivitas *reconnaissance*. Aktifitas tersebut dilakukan untuk menentukan serangan yang efektif.	Bila terdeteksi adanya kegiatan tersebut (persiapan DoS), maka organisasi harus memblokir trafik tersebut dengan mengubah aturan keamanan yang diterapkan, misalnya firewall memblokir sumber trafik bila protokol tertentu digunakan.
Keluarnya perangkat lunak untuk DoS versi baru dapat membahayakan organisasi.	Bila versi baru keluar, segera investigasi perangkat lunak tersebut, ubah kontrol keamanan sistem agar perangkat lunak tersebut tidak dapat bekerja dengan baik menyerang sistem di perusahaan.

Table 2: Tanda serangan DoS

Sedangkan pada tabel (3), menunjukkan aksi mencurigakan yang mungkin terhadap indikasi yang ada. Aksi mencurigakan yang dapat terjadi diantaranya DoS berbasis jaringan [1], dan DoS lokal [2].

Tabel (2) dan (3) bermanfaat dalam menganalisa insiden. Namun, ada komponen penting yang tidak ada dalam tabel tersebut, yaitu indikasi aktivitas yang "ramah" (*benign activity*). Aktivitas yang ramah tersebut memiliki gejala yang mirip dengan serangan DoS (misal tiba-tiba koneksi internet putus), sehingga orang yang menangani insiden kesulitan menentukan apakah sistemnya terkena insiden atau tidak. Oleh karena itu, aktivitas yang ramah ini tentunya harus dimasukkan ciri-cirinya ke dalam tabel agar orang yang sedang menganalisa insiden dapat membedakan apakah telah terjadi insiden atau tidak.

Analisis serangan DoS memiliki beberapa tantangan, diantaranya adalah:

1. Biasanya serangan DoS menggunakan protokol yang *connectionless* (UDP dan ICMP) atau protokol *connection-orriented* namun koneksi yang sepenuhnya tidak terjadi (misal TCP SYN pada serangan *Synflood*). Selain itu, mudah bagi penyerang memalsukan alamat IP nya sehingga tim penanganan insiden akan kesulitan mencari tahu sumber serangan yang sesungguhnya. ISP mungkin dapat membantu menelusuri serangan yang terjadi, namun akan lebih cepat bila dari organisasi yang bersangkutan yang menelusuri log yang ada terutama terkait dengan kegiatan *reconnaissance* (tahap awal penyerangan). Pada saat penyerang melakukan kegiatan tersebut, karena penyerang ingin mengetahui target yang diserang, biasanya penyerang ini menggunkan alamat asli. Hal tersebut tentunya dapat menjadi petunjuk dalam menelusuri siapa penyerang yang sesungguhnya.
2. Serangan DDoS biasanya menggunakan ratusan atau bahkan ribuan komputer yang menyerang. Komputer-komputer tersebut bisa dikendalikan oleh seseorang atau bahkan tidak dikendalikan secara langsung. Dengan begitu, komputer korban tidak akan dapat menelusuri siapakan penyerang yang sesungguhnya. Kemungkinan besar hanya dapat diketahui komputer yang telah dirasuki oleh penyerang untuk melakukan serangan DoS tanpa sadar.
3. Serangan DoS berbasis jaringan sulit dideteksi dengan baik oleh sensor IDS. Misalkan pada serangan synflood meski hanya mengirimkan sebuah

[1] DoS yang dilakukan melalui remote komputer [7]
[2] DoS yang biasanya berasal dari software berbahaya yang tertanam di komputer lokal [7]

Aksi Mencurigakan	Indikasi yang mungkin
DoS berbasis jaringan terhadap host tertentu	• Pengguna melapor sistem tidak dapat diakses • Tiba-tiba koneksi hilang • Peringatan dari *Network* IDS (NIDS) maupun *Host* IDS (HIDS) • Penggunaan *Bandwidth* jaringan yang meningkat dari biasanya • Adanya akses yang besar ke sebuah *host*, trafik jaringan yang tak simetris • Catatan log pada *firewall* dan *router* • Adanya paket dengan alamat sumber yang tidak biasa
DoS berbasis jaringan terhadap jaringan	• Pengguna melaporkan sistem dan jaringan tidak tersedia • Tiba-tiba koneksi hilang, peringatan dari NIDS • Penggunaan *Bandwidth* jaringan yang meningkat dari biasanya • Pola trafik jaringan yang tak simetris • Catatan log pada *firewall* dan *router* • Adanya paket dengan alamat sumber yang tidak biasa • Adanya paket dengan alamat tujuan yang tidak ada
DoS terhadap sistem operasi host tertentu	• Laporan sistem & aplikasi di komputer tidak dapat digunakan • Peringatan dari NIDS dan HIDS • Log dari sistem operasi • Adanya paket dengan alamat sumber yang tidak jelas
DoS terhadap aplikasi tertentu pada host tertentu	• Laporan aplikasinya tidak dapat digunakan • Peringatan dari NIDS dan HIDS • Log dari aplikasi • Adanya paket dengan alamat sumber yang tidak jelas

Table 3: Indikasi serangan DoS

request SYN ke tiap port, biasanya IDS akan mendeteksinya sebagai DoS. Bila server crash, pengguna yang akan mengaksesnya biasanya akan terus mengirimkan paket SYN menunggu agar bisa terhubung. Terkadang, koneksi dari pengguna yang berhak tersebut dideteksi sebagai serangan DoS oleh IDS.

4. Terkadang bila serangan DoS telah berhasil membuat sistem tidak tersedia, administrator berfikir kalau penyebabnya adalah ketidakstabilan dari sistem operasi yang digunakan. Oleh karena itu, biasanya sistem hanya akan direstart dan sementara sisem akan terlihat berjalan normal lagi. Hal tersebut terkadang menyebabkan administrator sistem tidak sadar akan adanya serangan.

3.3. Tahap Penanganan dan Pemulihan

Penanganan dan pemulihan dari serangan DoS yaitu harus menghentikan serangan DoS itu sendiri. Cara paling mudah adalah dengan memblokir seluruh trafik yang terindikasi melakukan serangan DoS. Namun, hal ini dapat diatasi oleh penyerang dengan cara memalsukan alamat IPnya sehingga serangan dapat dilanjutkan kembali. Solusi lainya dalam menangani serangan DoS adalah sebagai berikut.

1. Perbaiki kerentanan atau kelemahan yang ada di sistem yang digunakan sebagai sumber serangan. Misalkan, serangan terjadi karena *filtering* dari paket tidak memblokir paket yang menggunakan port 7 UDP (echo), dan port tersebut dapat diakses bebas oleh orang luar organisasi. Oleh karena itu, tutup koneksi ke port tersebut. Bila kerentanan ada pada sisi sistem operasi, maka lakukanlah *update* sistem segera.
2. Terapkan *filtering* yang berdasarkan karakteristik dari serangan. Strategi yang cukup baik diterapkan misalnya adalah pembatasan *rate* dari trafik yaitu hanya dapat mengirimkan paket dengan jumlah tertentu dalam suatu waktu pada protokol tertentu atau dalam melakukan hubungan dengan *host* tertentu. Meskipun begitu, pengaplikasian dari teknik *filtering* ini harus di lakukan pada tempat yang sesuai agar dampak buruk (misalkan performa yang turun, dan lainya) yang mungkin terjadi dapat diminimalisir.
3. Pastikan ISP yang digunakan mengimplementasikan *filtering* paket agar tidak semua *filtering* dilakukan oleh router organisasi.
4. Relokasi komputer yang menjadi target. Komputer yang sedang diserang, dapat direlokasi dengan mengganti alamat IP. Selain itu layanan yang

sedang diserang dapat dipindahkan pada *host* lain yang kalau bisa tidak memiliki kerentanan yang sama dengan *host* yang sebelumnya.

5. Serang si penyerang. Walaupun cara ini terkadang dapat menyerang pihak yang tidak bersalah karena si penyerang memalsukan alamat IPnya. Cara ini sebaiknya tidak dilakukan.

Tim penanganan insiden sebaiknya membuat tahapan solusi yang akan diimplementasikan bila serangan terjadi. Setelah serangan ditangani, tim penanganan insiden harus mengumpulkan bukti-bukti dan penanganan dari serangan DoS meskipun terkadang sulit dan memakan waktu karena beberapa alasan berikut.

1. Mengidentifikasi sumber serangan dari trafik yang diamati. Kesulitanya adalah IP penyerang yang dapat dengan mudah di palsukan.
2. Menelusuri kembali serangan melalui data yang ada di ISP. Hal ini terkadang sangat sulit ditelusuri bila serangan DoS telah selesai dibandingkan serangan yang masih berjalan. Terkadang ISP juga tidak dapat diajak kerja sama dengan pengguna layanan yang ingin menelusuri serangan yang telah terjadi.
3. Pelajari bagaimana *host* dapat diserang. Kesulitanya adalah pada serangan DDoS, penyerangan dilakukan oleh agen yang biasanya telah di bobol oleh penyerang pada waktu lampau.
4. *Review* log. Biasanya log yang harus direview berjumlah sangat banyak karena serangan DoS menghabiskan sumber daya sehingga membuat munculnya log baru.

3.4. Tahap Pasca Insiden

Tahap ini merupakan tahap yang dilakukan setelah insiden ditangani. Pada tahap ini, tim penanganan insiden harus membuat laporan penyelesaian insiden dan juga mengambil pelajaran dari insiden yang telah terjadi misalnya dengan mengadakan diskusi dengan pihak yang terlibah dalam penanganan insiden.

4. Kesimpulan

Penanganan insiden DoS memang tidak mudah, namun dapat dilakukan meskipun terkadang memakan banyak waktu dan sumber daya dalam penangananya. Beberapa poin penting rekomendasi dari NIST 800-61 terhadap penanganan insiden DoS adalah sebagai berikut.

1. Konfigurasi *rules* pada *firewall* untuk mencegah serangan reflektor.

2. Konfigurasi router yang berperan sebagai *gateway* untuk menolak setiap serangan penguatan.
3. Pastikan ISP yang digunakan oleh organisasi dapat membatu menangani insiden DoS yang berbasis jaringan.
4. Konfigurasi perangkat lunak keamanan untuk mendeteksi serangan DoS.
5. Konfigurasi perangkat jaringan yang ada di perbatasan jaringan internal dan eksternal agar menolak semua trafik yang datang dan masuk bila tidak diizinkan dengan jelas.
6. Buat strategi penanganan dengan menyertakan beberapa solusi yang bertahap akan dicoba.

Dengan penanganan yang baik dan benar sesuai dengan rekomendasi dari NIST 800-61, diharapkan agar insiden DoS dapat ditangani dengan lebih efektif dan efisien.

Referensi

[1] Paul Cichonski, dkk, "*Special Publication 800-61 Revision 2 Computer security incident handling guide*: *Recomendation of the National Institute of Standards and Technology*". Government Printing Office, Gaithersburg U.S. , 2012.

[2] Budi Rahardjo, "*Keamanan Sistem Informasi Berbasis Internet, versi 5.4*". PT Insan Infonesia - Bandung & PT INDOCISC, 2005.

[3] Simson Garfinkel, "*PGP: Pretty Good Privacy*," O'Reilly & Associates, Inc., 1995.

[4] ISACA Volunteer Member, "*Cybersecurity Fundamentals Study Guide*",ISACA, 2015.

[5] Tim Grance, dkk, "*Special Publication 800-61 Computer Security Incident Handling Guide : Recomendation of the National Institute of Standards and Technology*", Government Printing Office, Gaithersburg U.S. , 2004.

[6] Ahmad Alkazimy, "*Incident Handling ID-CERT",* Bandung, 2016

[7] Timothy John McNevin, "*Mitigating Network-Based Denial of Service Attacks with Client Puzzles: Thesis Virginia Polytechnic Institute and State University* ", Blacksburg, 2005