Angkasa Pura | AIRPORTS

PANDUAN

Penanganan Insiden Distributed Denial of Services (DDos)

ANGKASA PURA 1
COMPUTER SECURITY INCIDENT RESPONSE TEAM
(AP 1 - CSIRT)

KATA PENGANTAR

Puji syukur kehadirat Allah SWT, Tuhan Yang Maha Esa, atas segala limpahan rahmat, nikmat serta karunia-Nya yang tak ternilai dan tak dapat dihitung sehingga kami dapat menyelesaikan penyusunan “Panduan Penanganan Insiden DDoS”. Panduan ini disusun dalam rangka memberikan acuan bagi pihak yang berkepentingan dalam penanganan insiden serangan DDoS. Panduan ini berisikan langkah-langkah yang harus diambil apabila terjadi serangan DDoS, yang dimulai dari tahap persiapan sampai dengan tahap pembuatan laporan dari penanganan serangan. Panduan ini tentu saja masih banyak kekurangan dan masih jauh dari kesempurnaan karena keterbatasan ilmu dan referensi kami. Untuk itu, kami selalu berusaha melakukan evaluasi dan perbaikan secara berkala agar bisa mencapai hasil yang lebih baik lagi.

Akhir kata, kami ucapkan terima kasih kepada segala pihak yang telah membantu dalam penyusunan panduan ini.

Jakarta, 2023

ANGKASA PURA 1-CSIRT,

KETUA ANGKASA PURA 1-CSIRT

DAFTAR ISI

PANDUAN PENANGANAN INSIDEN
SERANGAN DISTRBUTED DENIAL OF SERVICE (DDoS)

1. PENDAHULUAN

Denial of Service (DoS) merupakan tipe serangan pada jaringan yang bertujuan agar suatu layanan tidak dapat digunakan atau bekerja secara normal. Pada serangan DoS biasanya *Attacker* akan mengirimkan trafik data / permintaan kepada target dengan jumlah yang besar yang bertujuan membebani sistem /kapasitas dari suatu *server* atau perangkat.

Distributed Denial of Service (DDoS) merupakan pengembangan dari DoS dengan tujuan yang sama akan tetapi akan lebih berbahaya karena kali ini penyerang akan menggunakan ratusan atau ribuan perangkat yang sudah dijadikan sebagai *Botnet/zombie* yang pada saat bersamaan akan melakukan serangan sehingga akan lebih cepat dalam membuat suatu layanan *down.*

2. TUJUAN

Secara umum, tujuan panduan ini dimaksudkan untuk membantu organisasi memiliki manajemen yang efektif dalam penanganan serangan DDoS pada jaringan komputer. Sedangkan secara khusus adalah sebagai berikut:

a) Memastikan adanya sumber daya yang memadai untuk menangani serangan yang terjadi;
b) Melakukan pengumpulan informasi yang akurat;
c) Meminimalisir dampak dari serangan yang terjadi;
d) Mencegah adanya serangan lanjutan dan mencegah kerusakan agar tidak lebih meluas.

3. RUANG LINGKUP

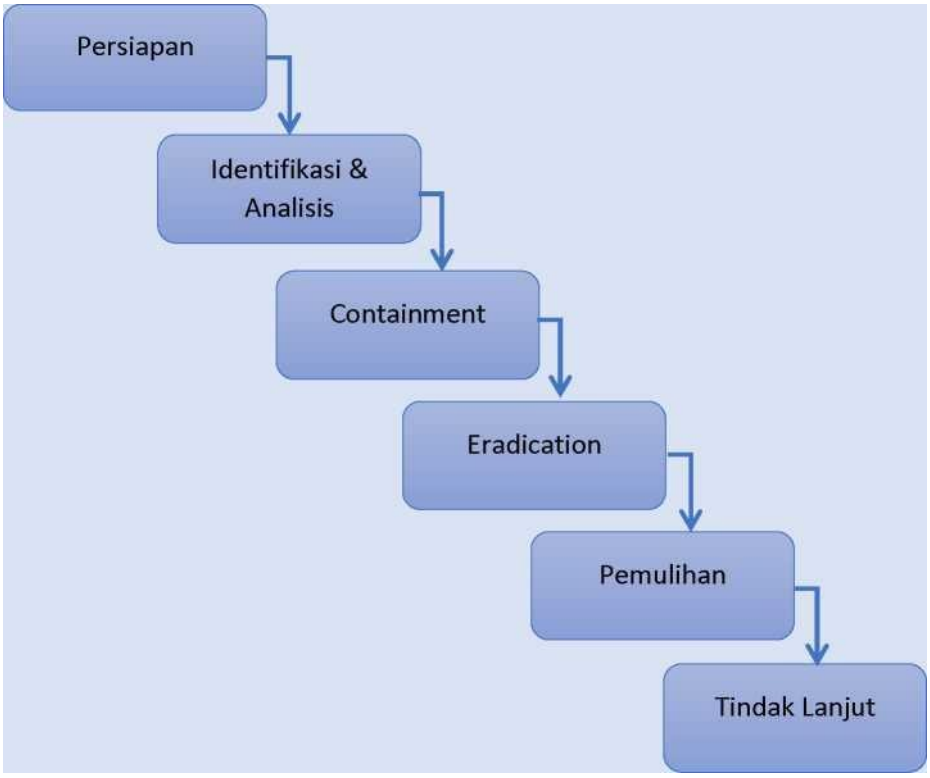
Panduan ini berisi langkah-langkah yang harus diambil apabila terjadi serangan DDoS, yang dimulai dari tahap persiapan sampai dengan tahap pembuatan laporan dari penanganan serangan. Serangan DDoS dapat terjadi pada semua server yang terhubung ke internet. Panduan ini dapat dijadikan acuan bagi semua individu atau tim yang bertindak sebagai penanggungjawab/ administrator dari suatu *server.*

4. PROSEDUR PENANGANAN SERANGAN DDoS

Serangan DDoS pada prinsipnya sama seperti serangan DoS, akan tetapi trafik serangan DDoS yang dikirim berasal dari berbagai sumber yang berbeda. Oleh karena itu, dalam penanganan serangan DDoS perlu melibatkan *Internet Service Provider* (ISP). Penanganan terhadap serangan DDoS dilakukan dalam beberapa tahap sebagai berikut:

4.1. Tahap Persiapan

Tujuan tahap persiapan pada penanganan serangan DDoS adalah untuk membangun kontak dan mempersiapkan sumber daya yang dibutuhkan untuk penanganan serangan DDoS.



Gambar 1. Tahap Penanganan Serangan DDoS

Tahap persiapan penanganan serangan DDoS, dilakukan dengan prosedur sebagai berikut:

a) Pembentukan tim respon. Tim dapat berasal dari institusi yang mengalami serangan (internal) atau juga bisa berasal dari luar institusi (eksternal) jika memang diperlukan. Anggota tim memiliki pengetahuan tentang DDoS dan memiliki kemampuan penanganannya.
b) Membangun kontak dengan ISP. Menentukan metode koordinasi dan komunikasi antara tim, penanggung jawab server, ISP dan pihak terkait. Kapan koordinasi harus dilakukan, dan melalui media komunikasi apa yang akan digunakan, misalkan telepon dan *email.*
c) Menyiapkan dokumen yang dibutuhkan dalam proses penanganan serangan DDoS. Dokumen ini antara lain adalah :
    - Panduan penanganan insiden siber
    - Formulir penanganan insiden siber
    - Dokumen yang berisi daftar dari alamat IP yang diprioritaskan untuk diperbolehkan melewati jaringan selama penanganan
    - Dokumen topologi jaringan, termasuk semua alamat IP yang paling *up to date.*
    - *Dokumen* Baseline Performance.
d) Menyiapkan *tools* yang diperlukan dalam proses penanganan, antara lain:
    - Perangkat Analisa Jaringan, misalnya wireshark, kfsensor, dll.
    - Perangkat Analisa *Log,* misalnya Notepad++/EmEditor, dll.
e) Mempersiapkan desain jaringan dengan menggunakan redundan di sisi perangkat, *server,* dan interkoneksi.
f) Melakukan *backup* secara berkala.

4.2. Identifikasi dan Analisis

Tujuan dari proses identifikasi adalah:

a) Memahami sifat dan ruang lingkup serangan.
b) Mengumpulkan informasi yang cukup tentang serangan sehingga tim respon dapat memprioritaskan langkah selanjutnya dalam menangani serangan tersebut. Kemampuan untuk mengidentifikasi dan memahami

sifat dari serangan dan target akan membantu dalam proses *containment* dan pemulihan. Langkah-langkah yang dapat diambil pada tahap identifikasi dan analisis antara lain:

i. Mengetahui perilaku "normal" dari lalu lintas jaringan, penggunaan CPU, penggunaan memori dari *host,* sehingga alat *monitoring* jaringan akan memberikan informasi berupa peringatan terhadap perubahan abnormal. Beberapa indikasi bahwa telah terjadi serangan DDoS diantaranya:
   - Melambatnya lalu-lintas jaringan
   - Melambatnya proses pada komputer *host*
   - Penggunaan ruang *disk* yang bertambah
   - Layanan tidak dapat diakses atau sistem *crash*
   - Waktu *login* yang lama, bahkan ditolak
   - *Log* penuh
   - Anomali pada fungsi *port*

ii. Mengidentifikasi komponen infrastruktur yang terkena dampak.

iii. Berkoordinasi dengan pihak terkait untuk mengetahui apakah jaringan organisasi merupakan target utama atau korban dari imbas (misalnya imbas dari serangan terhadap penyedia layanan internet atau penyedia *hosting*).

iv. Memeriksa lalu lintas jaringan, seperti *source IP address, destination port, URLs, protocol, TCP sysnc, UDP, ICMP* dan *traffic Netflow* misalnya menggunakan tcpdump, wireshark, snort dan membandingkannya dengan lalu lintas jaringan "normal". Dengan memeriksa lalu lintas jaringan, juga dapat diketahui sumber dan jenis serangan.

v. Menganalisa *file log* yang tersedia (*file log server*, *router*, *firewall*, aplikasi dan infrastruktur lainnya yang terkena dampak) untuk mengetahui jenis serangan, sumber serangan, apa yang menjadi sasaran, dan bagaimana masuknya serangan.

vi. Menentukan dampak dari tingkat keparahan yang terjadi, yaitu seberapa besar sistem dan layanan mengalami gangguan, serta kemungkinan motif yang dilakukan oleh penyerang.

4.3. Containment

Tahap *containment* bertujuan untuk meminimalisir efek/dampak serangan pada sistem yang ditargetkan dan mencegah kerusakan lebih lanjut.

Prosedur yang dilakukan pada tahap ini adalah:

a) Jika sumber *bottleneck* berada pada fitur tertentu dari suatu aplikasi (dalam artian suatu aplikasi sedang menjadi target), maka perlu mempertimbangkan untuk menonaktifkan sementara aplikasi tersebut.

b) Jika *bottleneck* berada di ISP, maka perlu berkoordinasi dengan pihak ISP untuk meminta *filtering.*

c) Merelokasi target ke alamat IP lain jika suatu *host* tertentu sedang menjadi target (sebagai solusi sementara).

d) Jika memungkinkan, memblokir lalu lintas yang terhubung dengan jaringan *(router, firewall, load balancer,* dll).

e) Mengontrol lalu lintas data dengan menghentikan koneksi atau proses yang tidak diinginkan pada *server/router.*

f) Melakukan *filter* sesuai karakteristik serangan, misalnya memblokir paket *echo* ICMP.

g) Menerapkan *rate limiting* untuk protokol tertentu, mengijinkan dan membatasi jumlah paket per detik untuk protokol tertentu dalam mengakses suatu *host*.

4.4. Eradication

Eradication pada penanganan serangan DDoS yaitu mengambil tindakan untuk menghentikan kondisi *denial of service.* Tindakan ini sebagaian besar melibatkan peran ISP.

Prosedur untuk melakukan proses ini dapat dilakukan dengan cara menghubungi penyedia layanan internet (ISP) untuk meminta bantuan, terkait:

- Pemblokiran jaringan *(source IP address)*
- Pemfilteran (membatasi jumlah lalu lintas)

- *Traffic-scrubbing/shinkhole/clean-pipe*
- *Blackhole routing*

4.5. Pemulihan

Pemulihan merupakan tahap untuk mengembalikan seluruh sistem bekerja normal seperti semula. Memahami karakteristik serangan diperlukan untuk pemulihan yang cepat dan tepat. Prosedur yang dapat dilakukan pada tahap pemulihan diantaranya sebagai berikut:

a) Memastikan bahwa serangan DDoS pada jaringan telah selesai dan layanan bisa dilakukan kembali.
b) Memastikan bahwa jaringan telah kembali ke kinerja semula
c) Memastikan bahwa layanan yang terkena dampak dapat dijangkau lagi/beroperasi kembali.
d) Memastikan bahwa infrastruktur telah kembali ke kinerja semula (tidak ada kerusakan)
e) Memulai layanan, aplikasi dan modul yang ditangguhkan
f) Mengembalikan ke jaringan asli dan mengalihkan kembali lalu lintas ke jaringan asli.

4.6 Tindak Lanjut

Tahap ini adalah fase di mana semua dokumentasi kegiatan yang dilakukan dicatat sebagai referensi untuk di masa mendatang. Tujuan dari tahap ini adalah untuk:

a) Pelaporan, membuat laporan mengenai langkah-langkah dan hasil yang telah didapatkan pada penanganan serangan DDoS.
b) Mengambil pelajaran dan membuat rekomendasi untuk mencegah terjadi lagi. Prosedur yang dapat dilakukan adalah sebagai berikut:
    i. Membuat dokumentasi dan laporan terkait penanganan serangan DDoS, yang berisi langkah-langkah dan hasil yang telah didapatkan pada penanganan serangan DDoS. Mendokumentasikan dampak dan biaya dari terjadinya serangan tersebut.
    ii. Evaluasi efektivitas respon

iii. Menyempurnakan langkah-langkah respon, prosedur penanganan serangan yang diambil selama insiden
iv. Mencatat *tools* apa saja yang digunakan dalam penanganan.
v. Mendokumentasikan bukti-bukti yang ditemukan, hal ini terkait dengan proses hukum kedepannya.
vi. Memberikan analisa dan penjelasan apa yang harus dilakukan sehingga serangan serupa tidak terulang kembali.
vii. Membuat evaluasi dan rekomendasi.