DISKOMINFO BATAM

G20 INDONESIA 2022

BerAKHLAK
Berorientasi Pelayanan Akuntabel Kompeten Harmonis Loyal Adaptif Kolaboratif

PANDUAN PENANGANAN INSIDEN SERANGAN

DISTRIBUTED DENIAL OF SERVICE (DDOS)

Dinas Komunikasi dan Informatika Kota Batam

Distributed Denial of Service
(DDOS) Attack

DISKOMINFO BATAM

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) 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

DISKOMINFO BATAM

G20 INDONESIA 2022

BerAKHLAK
Berorientasi Pelayanan Akuntabel Kompeten Harmonis Loyal Adaptif Kolaboratif

TUJUAN

1. Memastikan adanya sumber daya yang memadai untuk menangani serangan yang terjadi
2. Melakukan pengumpulan informasi yang akurat
3. Meminimalisir dampak dari serangan yang terjadi
4. Mencegah adanya serangan lanjutan dan mencegah kerusakan agar tidak lebih meluas

DISKOMINFO BATAM

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

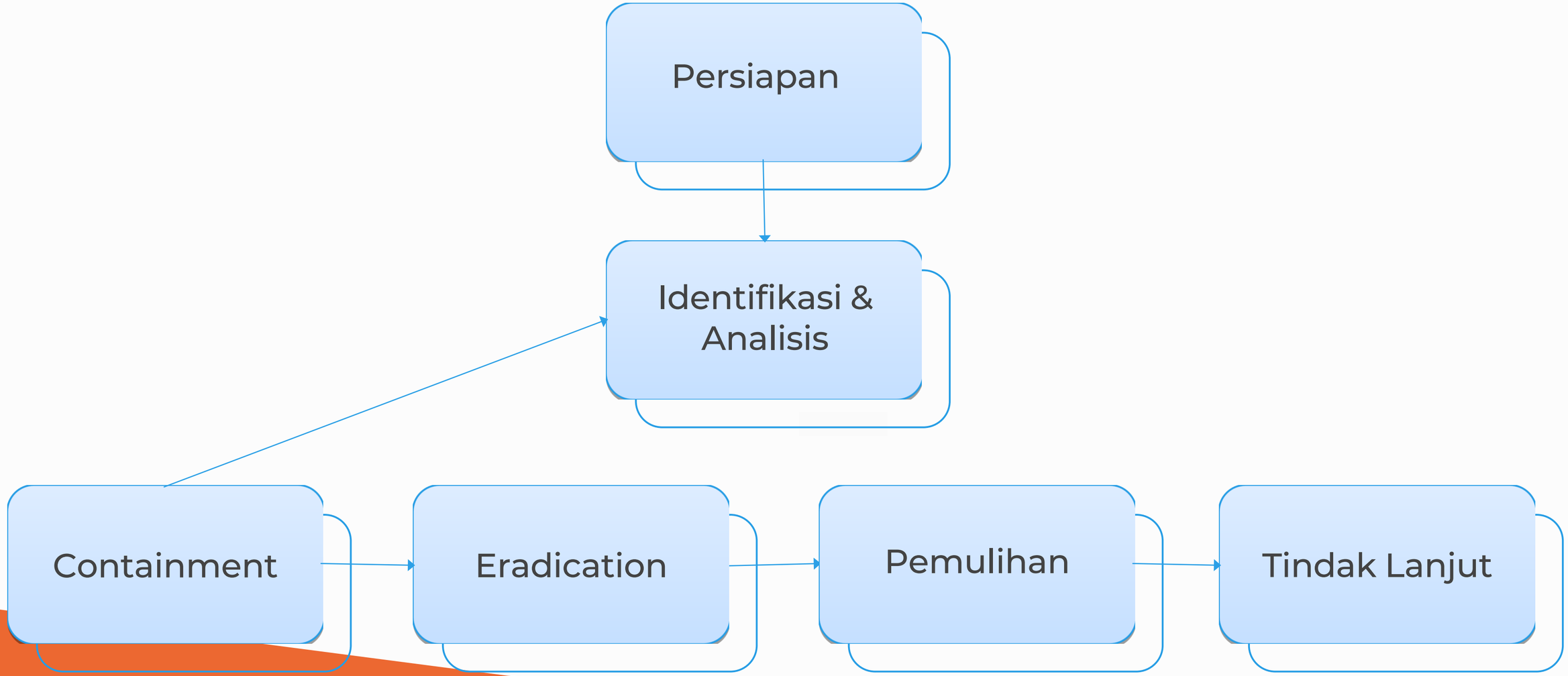
Serangan DDoS dapat terjadi pada semua server yang terhubung ke internet. Panduan ini dapat dijadikan acuan bagi semua individu atau tim yang bertindak sebagai penanggungjawab/administrator dari suatu server

G20 INDONESIA 2022

BerAKHLAK
Berorientasi Pelayanan Akuntabel Kompeten Harmonis Loyal Adaptif Kolaboratif

DISKOMINFO BATAM

PROSEDUR PENANGANAN SERANGAN DDOS



TAHAP PERSIAPAN

1. 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

2. 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

3. 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

TAHAP PERSIAPAN

4 Menyiapkan tools yang diperlukan dalam proses penanganan, antara lain:

- Perangkat Analisa Jaringan, misalnya wireshark, kfsensor
- Perangkat Analisa Log, misalnya Notepad++/EmEditor

5 Mempersiapkan desain jaringan dengan menggunakan redundan di sisi perangkat, server, dan interkoneksi

6 Melakukan backup secara berkala

IDENTIFIKASI DAN ANALISIS

TUJUAN

1. Memahami sifat dan ruang lingkup serangan

2. 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

1. 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

IDENTIFIKASI DAN ANALISIS

LANGKAH-LANGKAH

2. Mengidentifikasi komponen infrastruktur yang terkena dampak

3. 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)

4. 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

5. 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

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

DISKOMINFO BATAM

CONTAINMENT

G20 INDONESIA 2022

BerAKHLAK
Berorientasi Pelayanan Akuntabel Kompeten Harmonis Loyal Adaptif Kolaboratif

01

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

02

Jika bottleneck berada di ISP, maka perlu berkoordinasi dengan pihak ISP untuk meminta filtering

03

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

04

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

DISKOMINFO BATAM

CONTAINMENT

G20 INDONESIA 2022

BerAKHLAK
Berorientasi Pelayanan Akuntabel Kompeten Harmonis Loyal Adaptif Kolaboratif

05 Mengontrol lalu lintas data dengan menghentikan koneksi atau proses yang tidak diinginkan pada server/router

06 Melakukan filter sesuai karakteristik serangan, misalnya memblokir paket echo ICMP

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

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

Atara lain

1. Pemblokiran jaringan (source IP address)
2. Pemfilteran (membatasi jumlah lalu lintas)
3. Traffic-scrubbing/shinkhole /clean-pipe
4. Pemblokiran jaringan (source IP address)

PEMULIHAN

Pemulihan merupakan tahap untuk mengembalikan seluruh sistem bekerja normal seperti semula

Prosedur

1. Memastikan bahwa serangan DDoS pada jaringan telah selesai dan layanan bisa dilakukan kembali
2. Memastikan bahwa jaringan telah kembali ke kinerja semula
3. Memastikan bahwa layanan yang terkena dampak dapat dijangkau lagi/beroperasi kembali
4. Memastikan bahwa infrastruktur telah kembali ke kinerja semula (tidak ada kerusakan)
5. Memulai layanan, aplikasi dan modul yang ditangguhkan
6. Mengembalikan ke jaringan asli dan mengalihkan kembali lalu lintas ke jaringan asli

TINDAK LANJUT

Tahap ini adalah fase di mana semua dokumentasi kegiatan yang dilakukan dicatat sebagai referensi untuk di masa mendatang

TUJUAN

1. Pelaporan, membuat laporan mengenai langkah-langkah dan hasil yang telah didapatkan pada penanganan serangan DDoS
2. Mengambil pelajaran dan membuat rekomendasi untuk mencegah terjadi lagi

PROSEDUR

1. Membuat dokumentasi dan laporan terkait penaganan DDoS, yang berisi langkah-langkah dan hasil yang telah didapatkan pada penanganan serangan DDoS. Mendokumentasikan dampak dan biaya terjadinya serangan tersebut
2. Evaluasi efektivitas respon
3. Menyempurnakan langkah-langkah respon, prosedur penanganan serangaan yang diambil dalam insiden
4. Mencatat tools apa saja yang digunakan dalam penanganan
5. Mendokumentasikan bukti-bukti yang ditemukan, hal ini terkait dengan proses hukum kedepannya
6. Memberikan analisa dan penjelasan apa yang harus dilakukan sehingga serangaan serupa tidak terulang kembali
7. Mendokumentasikan bukti-bukti yang ditemukan, hal ini terkait dengan proses hukum kedepannya

DISKOMINFO BATAM

G20 INDONESIA 2022

BerAKHLAK
Berorientasi Pelayanan Akuntabel Kompeten Harmonis Loyal Adaptif Kolaboratif

PANDUAN PENANGANAN INSIDEN SERANGAN

DISTRIBUTED DENIAL OF SERVICE (DDOS)

Dinas Komunikasi dan Informatika Kota Batam

Distributed Denial of Service
(DDOS) Attack