PEMERINTAH PROVINSI NUSA TENGGARA TIMUR

PANDUAN PENANGANAN INSIDEN SERANGAN DDoS

DETEKSI RESPON MITIGASI PEMULIHAN

DINAS KOMUNIKASI DAN INFORMATIKA
PROVINSI NUSA TENGGARA TIMUR

BIDANG PERSANDIAN DAN PENGAMANAN INFORMASI

KATA PENGANTAR

Puji syukur kami panjatkan ke hadirat Allah SWT atas segala rahmat dan karunia-Nya sehingga penyusunan "Panduan Penanganan Insiden Serangan DDoS" ini dapat diselesaikan. Panduan ini dibuat sebagai acuan bagi seluruh pihak yang berkepentingan dalam menghadapi insiden serangan DDoS. Di dalamnya tertuang langkah-langkah konkret yang perlu ditempuh saat serangan DDoS terjadi, mulai dari kesiapan awal hingga pelaporan akhir pasca penanganan.

Kami menyadari bahwa panduan ini masih memiliki ruang untuk penyempurnaan. Oleh karena itu, evaluasi dan pembaruan berkala akan terus dilakukan demi meningkatkan kualitasnya.

Ucapan terima kasih kami sampaikan kepada semua pihak yang telah berkontribusi dalam penyusunan panduan ini.

Kupang, 08 Mei 2026
Kepala Dinas Komunikasi dan Informatika
Provinsi Nusa Tenggara Timur,

Drs. Ady Endezon Mandala, M.Si
Pembina Utama Muda
NIP. 197001231990091002

DAFTAR ISI

PROSEDUR PENANGANAN INSIDEN DENIAL OF SERVICE (DOS)

1. PENDAHULUAN

Denial of Service (DoS) merupakan jenis serangan siber yang menargetkan ketersediaan layanan jaringan dengan cara membanjiri server atau perangkat menggunakan arus data atau permintaan berlebih, sehingga sistem tidak mampu beroperasi sebagaimana mestinya.

Distributed Denial of Service (DDoS) adalah bentuk lanjutan dari DoS yang jauh lebih mengancam. Pada serangan ini, pelaku menggerakkan ratusan hingga ribuan perangkat yang telah dikompromikan (botnet/zombie) secara serempak untuk melancarkan serangan, sehingga suatu layanan dapat dijatuhkan dalam waktu yang lebih singkat.

2. TUJUAN

Panduan ini bertujuan membantu organisasi membangun manajemen insiden yang efektif dalam menghadapi serangan DDoS. Secara spesifik, panduan ini ditujukan untuk:

- Memastikan ketersediaan sumber daya yang cukup dalam merespons serangan;
- Menjamin proses pengumpulan data dan informasi yang sahih dan akurat;
- Menekan dampak kerugian yang ditimbulkan oleh serangan semaksimal mungkin;
- Mencegah eskalasi serangan dan membatasi perluasan dampak yang terjadi.

3. RUANG LINGKUP

Panduan ini mencakup serangkaian prosedur yang perlu dijalankan ketika terjadi serangan DDoS, dari fase kesiapan awal hingga pelaporan akhir. Mengingat serangan DDoS berpotensi menimpa seluruh server yang terhubung ke internet, panduan ini dapat digunakan sebagai rujukan oleh setiap individu maupun tim yang mengemban tanggung jawab sebagai administrator server.

4. PROSEDUR PENANGANAN INSIDEN DDoS

Berbeda dengan DoS, serangan DDoS menggunakan banyak sumber lalu lintas secara bersamaan. Hal ini menjadikan penanganannya lebih kompleks dan memerlukan koordinasi dengan pihak Internet Service Provider (ISP). Prosedur penanganan dilakukan melalui enam tahapan yang berurutan:

Gambar 1. Alur Tahapan Penanganan Insiden DDoS

4.1. Persiapan

Tahap ini bertujuan membangun fondasi koordinasi dan memastikan seluruh sumber daya yang diperlukan siap tersedia sebelum insiden terjadi. Langkah-langkah yang perlu ditempuh meliputi:

1. Pembentukan tim respons insiden, baik dari internal organisasi maupun pihak eksternal yang relevan. Seluruh anggota tim wajib memahami karakteristik serangan DDoS dan mekanisme penanganannya.
2. Membangun jalur komunikasi dengan ISP dan menentukan skema koordinasi, termasuk metode dan media komunikasi yang akan digunakan (telepon, email, dsb.).
3. Menyiapkan dokumen-dokumen pendukung, antara lain:
   - Panduan dan formulir penanganan insiden siber
   - Daftar alamat IP yang diizinkan melintas selama proses penanganan
   - Dokumen topologi jaringan beserta daftar alamat IP terkini
   - Dokumen Baseline Performance

4. Mempersiapkan perangkat/tools teknis yang dibutuhkan, seperti alat analisa jaringan (Wireshark, Kfsensor) dan alat analisa log (Notepad++, EmEditor).
5. Merancang infrastruktur jaringan yang menerapkan redundansi pada perangkat, server, dan jalur interkoneksi.
6. Melaksanakan pencadangan data (backup) secara rutin dan terjadwal.

4.2. Identifikasi dan Analisis

Tujuan dari tahap ini adalah memahami karakteristik serangan secara mendalam dan mengumpulkan data yang cukup agar tim respons dapat menentukan prioritas langkah selanjutnya. Tahap identifikasi dan analisis mencakup:

1. Membangun pemahaman tentang kondisi normal jaringan—meliputi penggunaan CPU, memori, dan pola lalu lintas—sehingga sistem pemantauan dapat segera mendeteksi anomali. Beberapa indikator yang mengisyaratkan terjadinya serangan DDoS:
   - Lalu lintas jaringan mengalami perlambatan signifikan
   - Proses komputasi pada host berjalan lambat
   - Kapasitas disk meningkat secara tidak wajar
   - Layanan tidak dapat diakses atau sistem mengalami crash
   - Waktu login memanjang atau bahkan ditolak
   - File log terisi penuh
   - Ditemukan anomali pada fungsi port
2. Mengidentifikasi komponen infrastruktur yang terdampak.
3. Berkoordinasi dengan pihak terkait guna memverifikasi apakah organisasi merupakan target langsung atau hanya terkena dampak dari serangan terhadap penyedia layanan lain.
4. Memeriksa lalu lintas jaringan secara mendetail—mencakup source IP, port tujuan, URL, protokol, TCP sync, UDP, ICMP, dan Netflow—menggunakan tools seperti tcpdump, Wireshark, atau Snort, lalu membandingkannya dengan kondisi normal untuk menentukan sumber dan jenis serangan.
5. Menganalisis file log dari server, router, firewall, dan komponen infrastruktur lain yang terdampak guna menelusuri jenis, sumber, dan vektor masuk serangan.
6. Menentukan tingkat keparahan insiden, termasuk skala gangguan layanan yang dialami dan kemungkinan motif di balik serangan tersebut.

4.3. Containment

Tahap containment bertujuan membatasi dampak serangan terhadap sistem yang ditarget dan mencegah kerusakan meluas lebih jauh. Prosedur yang dapat diterapkan antara lain:

1. Apabila suatu aplikasi menjadi titik kelemahan (bottleneck), pertimbangkan untuk menonaktifkannya sementara waktu.
2. Jika bottleneck terjadi di sisi ISP, segera berkoordinasi dengan ISP untuk meminta penerapan filtering.
3. Merelokasi host yang menjadi target ke alamat IP berbeda sebagai solusi sementara.
4. Memblokir lalu lintas mencurigakan melalui perangkat jaringan seperti router, firewall, atau load balancer.
5. Menghentikan koneksi atau proses yang tidak diperlukan pada server maupun router.
6. Menerapkan filter berbasis karakteristik serangan, misalnya memblokir paket echo ICMP.
7. Memberlakukan rate limiting untuk protokol tertentu guna membatasi volume paket yang diizinkan mengakses suatu host per satuan waktu.

4.4. Eradication

Eradication merupakan tahap pengambilan tindakan definitif untuk menghentikan kondisi denial of service. Pada tahap ini, peran ISP sangat krusial. Prosedur yang dilakukan adalah dengan menghubungi ISP dan meminta bantuan berupa:

- Pemblokiran source IP address yang teridentifikasi sebagai sumber serangan
- Pembatasan volume lalu lintas (traffic filtering)
- Traffic scrubbing, sinkhole, atau clean-pipe untuk memisahkan lalu lintas bersih dari serangan
- Blackhole routing untuk membuang lalu lintas serangan sebelum mencapai target

4.5. Pemulihan

Pemulihan adalah tahap pengembalian seluruh sistem ke kondisi operasional normal. Pemahaman mendalam atas karakteristik serangan akan mempercepat dan mengefektifkan proses ini. Langkah-langkah pemulihan yang perlu dilakukan:

1. Memverifikasi bahwa serangan DDoS benar-benar telah berakhir dan layanan kembali dapat dioperasikan.
2. Memastikan performa jaringan telah pulih ke kondisi semula.

3. Memastikan seluruh layanan yang sebelumnya terdampak kini dapat diakses kembali.
4. Memastikan infrastruktur tidak mengalami kerusakan dan berfungsi normal.
5. Mengaktifkan kembali layanan, aplikasi, dan modul yang sempat ditangguhkan.
6. Mengembalikan konfigurasi jaringan ke kondisi asal dan mengalihkan kembali seluruh lalu lintas ke jalur jaringan semula.

4.6. Tindak Lanjut

Tindak lanjut merupakan fase akhir yang berfokus pada pendokumentasian seluruh aktivitas sebagai referensi dan bahan pembelajaran untuk masa mendatang. Tujuannya adalah menyusun laporan yang komprehensif dan merumuskan rekomendasi pencegahan insiden serupa. Prosedur yang dilakukan meliputi:

1. Menyusun dokumentasi dan laporan lengkap atas seluruh proses penanganan serangan DDoS, termasuk pencatatan dampak dan estimasi kerugian yang ditimbulkan.
2. Mengevaluasi efektivitas respons yang telah dijalankan.
3. Menyempurnakan prosedur dan langkah-langkah respons berdasarkan pelajaran yang dipetik dari insiden.
4. Mencatat seluruh tools yang digunakan selama proses penanganan berlangsung.
5. Mendokumentasikan bukti-bukti yang ditemukan untuk keperluan proses hukum di masa mendatang.
6. Memberikan analisis dan rekomendasi konkret guna mencegah terulangnya serangan serupa.

   Menyusun laporan evaluasi dan rekomendasi peningkatan keamanan secara