PANDUAN MENGHADAPI SERANGAN *DENIAL OF SERVICE (DOS)*

Untuk Badan Usaha Kecil dan Menengah

PUSAT OPERASI KEAMANAN SIBER NASIONAL

Ministry of Science and ICT

KISA KOREA INTERNET & SECURITY AGENCY

Panduan ini dipublikasikan oleh **Pusat Operasi Keamanan Siber Nasional (Pusopskamsinas) Badan Siber dan Sandi Negara (BSSN)** bekerja sama dengan **Cyber Shelter** (**Ministry of Science and ICT Korea** dan **Korea Internet & Security Agency)** untuk badan usaha kecil dan menengah dalam menangani serangan Distributed Denial of Service (DDoS).

DAFTAR ISI

Pusopskamsinas BSSN telah mendapat persetujuan utnuk mengalih bahasakan dokumen "Guidance on Responding to Denial of Service Attack (For SME)" sebagai bagian dari kerjasama dengan Ministry of Science and ICT Korea dan Korea Internet & Security Agency (KISA).
Dokumen asli:
https://www.boho.or.kr/filedownload.do?attach_file_seq=2354&attach_file_id=EpF2354.pdf

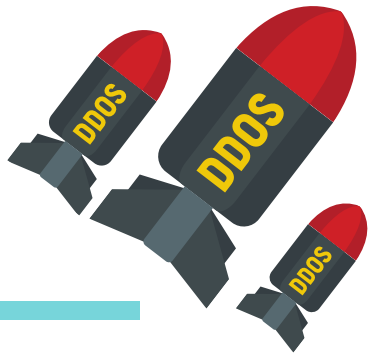
PUSAT OPERASI KEAMANAN SIBER NASIONAL

Ministry of Science and ICT

KISA KOREA INTERNET & SECURITY AGENCY

BAGIAN 1: PENDAHULUAN

Serangan DDoS? Apa itu?



Seperti namanya, "*denial*" yang berarti penolakan atau penyangkalan, **Denial of Service (DoS)** adalah serangan berupa percobaan untuk membuat jaringan atau sebuah sistem menolak untuk bekerja atau menjalankan layanannya.

Contohnya, sebuah *website* pasar *online* tidak bisa memberikan layanan karena ketika *website*-nya diakses, kita tidak dapat menggunakannya. Layanan dalam *website* tidak dapat ditampilkan, biasanya kita akan melihat *website* tersebut menampilkan keterangan seperti: *503 service unavailable*, yang berarti layanan tidak tersedia. Sebagai pengguna tentu kita akan merasa kesal jika *website* yang ingin kita kunjungi menunjukan halaman seperti ini. Bagi si pemilik *website* tentu ini lebih merugikan, apalagi jika *website* tersebut adalah tulang punggung usaha.

Bagaimana Serangan DoS Terjadi?

Bayangkan seorang penjual bubur ayam berjualan dengan gerobak. Ia memiliki 5 buah kursi untuk pelanggan duduk. Ia juga sudah siap dengan 20 buah mangkuk dan sendok, juga persediaan bubur ayam dan topping yang cukup untuk 100 mangkuk. Ia siap berjualan.

Ketika ia mendapat 5 orang pelanggan dan meminta dilayani secara bersamaan. Ia akan dengan cekatan membuatkan 5 mangkuk bubur ayam sekaligus. Bahkan jika permintaannya berbeda-beda. Ada yang ingin memakai sambal, ada yang tidak suka kecap manis, dan sebagainya. Ia dengan cekatan melayani 5 orang pelanggan yang datang bersamaan. Saat kelimanya pergi, ia melayani pelanggan berikutnya, terus-menerus silih berganti.

Suatu ketika ada seorang pelanggan datang dengan memesan bubur banyak sekali. Awalnya ia meminta dibuatkan 1 mangkuk bubur, saat si penjual baru saja membuka kuali, si pelanggan memesan lagi mangkuk ke-dua. Begitu seterusnya hingga si penjual kewalahan melayani si pelanggan ini. Ia bahkan tidak sadar bahwa bahan-bahan (persediaan mangkuk, bubur, dan bahan lainnya) tak cukup untuk melayani pesanan si pelanggan. Selain itu, pelanggan lain yang ingin membeli bubur jadinya tidak bisa membeli. Jangankan untuk membeli, berbicara pada si penjual bubur saja tidak bisa.

Begitulah bagaimana serangan DoS bekerja. Serangan ini dapat memperlambat sistem yang diserang, bahkan bisa merusaknya.

Siapa yang Menjadi Target Serangan DoS?

Serangan DoS memanfaatkan kelemahan sistem pada keterbatasan sumber daya, baik itu *bandwidth*, kemampuan menyimpan memori, server, dan lainnya. Sehingga kebanyakan DoS menyerang bisnis kecil hingga menengah yang tidak memiliki sumber daya yang cukup mewah. Pada dasarnya tujuan penyerang hanya untuk membuat sistem lumpuh, tapi tak jarang juga ada yang memanfaatkannya dengan menawarkan biaya tebusan untuk menghentikan serangan.

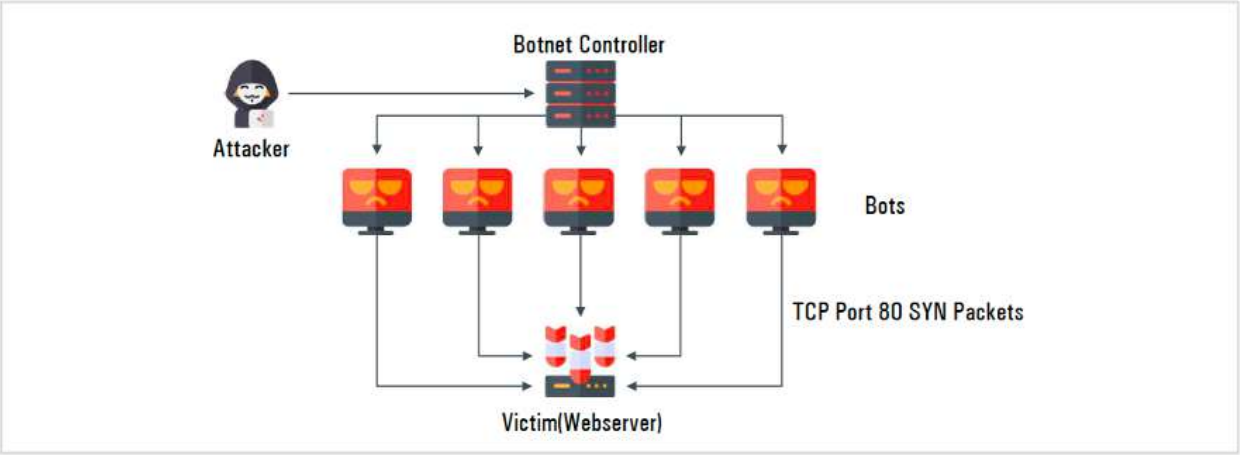
Apa Itu Serangan *DDoS*?

Ingat si pelanggan yang memesan banyak sekali bubur ayam hingga membuat si penjual kewalahan?

Dia adalah serangan DoS. Ketika ada banyak pelanggan yang bertingkah serupa, dan datang secara bersamaan, mereka adalah **Distributed Denial of Service (DDoS)**. Dalam serangan DoS, si penyerang menggunakan satu computer dan satu koneksi internet saja ketika meluncurkan serangan. Tetapi dalam DDoS, si penyerang menggunakan banyak computer dengan banyak koneksi internet yang ia kontrol secara bersamaan dengan menggunakan **botnet**.

Botnet adalah sejumlah komputer yang terinfeksi oleh malware tanpa disadari oleh penggunanya. Sebelum melancarkan aksi DDoS, si penyerang harus terlebih dahulu mengumpulkan tentara. Caranya adalah dengan menyebarkan malware sebanyak-banyaknya pada komputer dengan sistem keamanan yang buruk. Malware tersebut dapat memungkinkan si penyerang untuk mengontrol komputer yang terjangkit (*zombie host*). Katakanlah seorang penyerang telah berhasil mengaktifkan malware pada 10.000 komputer, program yang ia tanam telah masuk dan dalam keadaan tidur, namun siap untuk melancarkan aksi ketika diberi “aba-aba” oleh si penyerang.

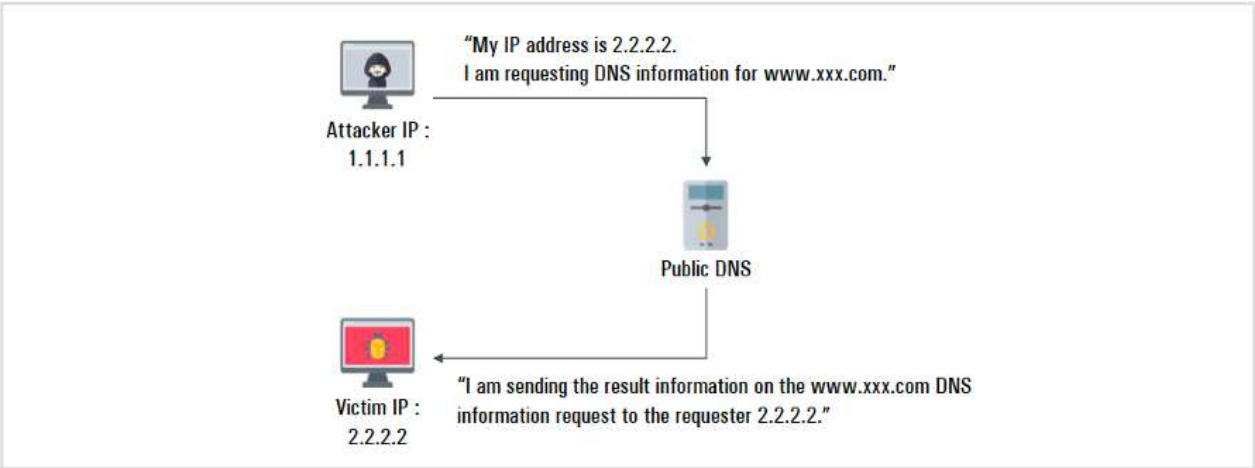
Dengan menggunakan botnet inilah si penyerang melakukan serangan DDoS. Karena berasal dari komputer dan koneksi internet yang berbeda-beda, DDoS semakin sulit untuk dideteksi dan dicegah, karena dianggap sebagai request biasa dari pengguna pada umumnya, bukan bot. Jumlah botnet yang dikontrol si penyerang bisa dalam jumlah besar karena malware sangat mudah menyebar bahkan hingga ke berbagai negara sekalipun.



Gambar 1.1 DDoS SYN Flood Attack

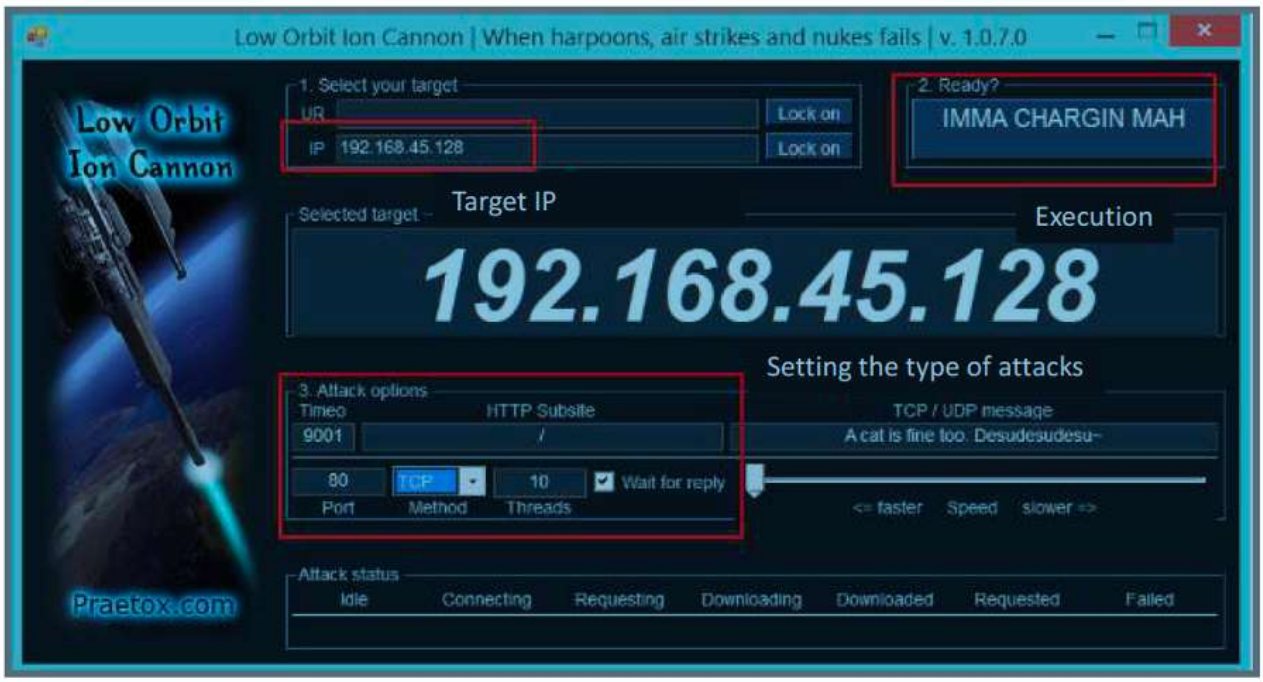
DDoS terjadi ketika si penyerang menggunakan alamat IP curian dari komputer zombie. Jika si penyerang menggunakan alamat IP dari komputer botnet ketika mengirimkan request service, maka webserver pun akan mengirim respon ke alamat IP si botnet. Di sisi lain, teknologi amplifikasi yang digunakan bersamaan dengan serangan, memungkinkan respon yang dikirimkan oleh webserver korban menjadi lebih banyak, sehingga hal ini membuat hasil serangan DDoS semakin efektif.

Terihat dalam gambar berikut bahwa si penyerang melakukan penipuan dengan menyamar sebagai si komputer botnet, lalu membuat request berbahaya kepada sebuah webserver. Meskipun penyerang mengirimkan request kecil, tapi si komputer botnet dapat menerima respons dengan jumlah besar.



Gambar 1.2 Contoh Serangan Refleksi dan Amplifikasi DNS

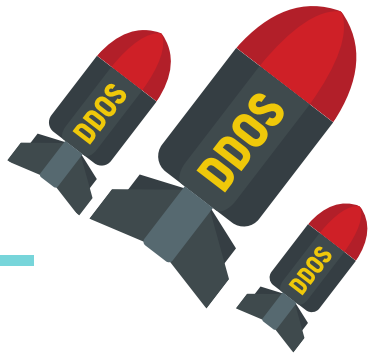
Saat ini pun, tools atau alat untuk melakukan serangan DDoS sudah mudah didapatkan, baik yang gratis maupun berbayar, di antaranya adalah Low Orbit Ion Cannon (LOIC) dan High Orbit Ion Cannon (HOIC), seperti yang terlihat dalam gambar berikut:



Gambar 1.3 Tampilan pada LOIC

BAGIAN 2:

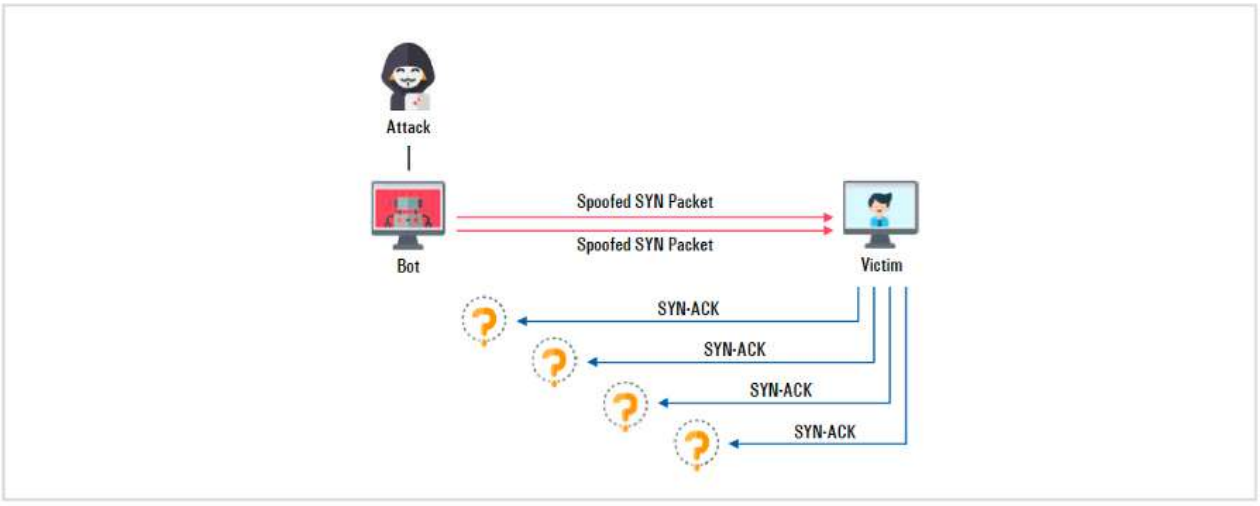
Jenis-Jenis Serangan DDoS



SYN Flood Attack

SYN Flood adalah jenis serangan DDoS yang paling tua, juga merupakan jenis serangan yang paling banyak digunakan. Penyerang mengirimkan permintaan koneksi ke TCP (SYN) secara terus-menerus kepada sistem milik korban, dengan tujuan untuk mengkonsumsi semaksimal mungkin kemampuan server korban. Ketika sebuah server menerima permintaan koneksi SYN, server akan membiarkan jalur komunikasi terbuka untuk menunggu langkah berikutnya yaitu pesan SYN-ACK (acknowledgement) dari client, yang berfungsi untuk mengkonfirmasi koneksi.

SYN Flood mengkonsumsi kemampuan server hingga tenggat waktu koneksi berakhir, karena sebenarnya serangan ini tidak mengirimkan SYN-ACK. Hasilnya, server victim tidak bisa membuka koneksi untuk pengguna / client lain (bukan penyerang), yang membuat mereka tidak dapat menggunakan layanan dari server.



Gambar 2.1.Gambaran SYN Flood Attack

Tindakan Penanggulangan

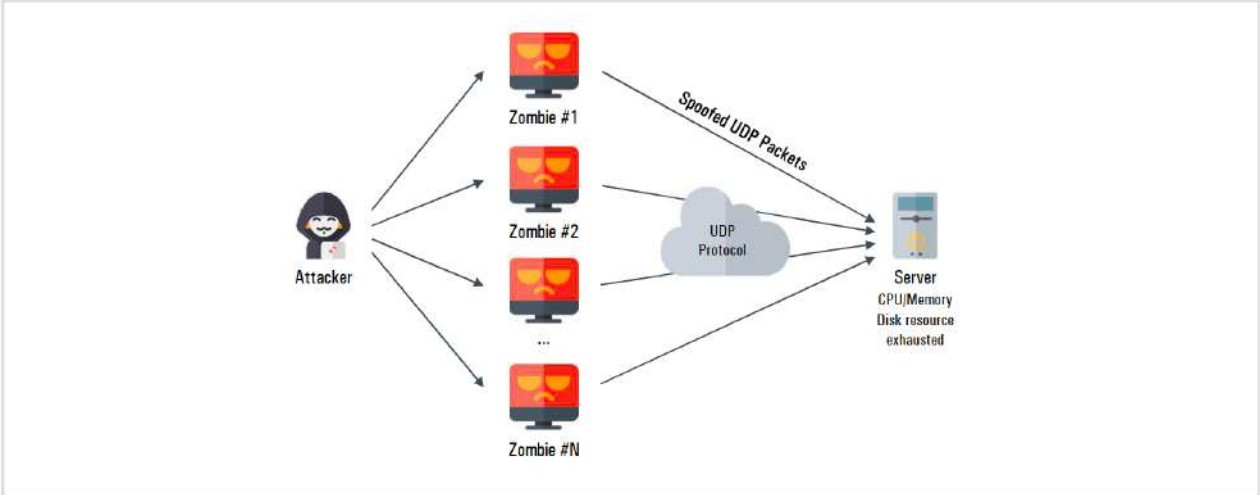
- Periksa network log, kemudian cari TCP SYN flag untuk memeriksa apakah ada terjadi SYN Flood. Untuk melakukan ini kita dapat menggunakan tools seperti TCPdump atau Wireshark.
- Paket TCP SYN sebenarnya normal dan tidak menunjukan indikasi aktivitas mencurigakan. Bagaimanapun hal ini bisa dianggap sebagai serangan DDoS jika beberapa paket SYN terbentuk dalam periode waktu yang singkat.

- Jika telah terdeteksi adanya sebuah serangan, kirim permintaan penaggulangan kepada network service provider (IPS, dll) untuk melakukan mitigasi terhadap serangan.
- Mendefinisikan rule “TCP Keepalive” dan “maximum connection” di semua perangkat terkait seperti: firewall dan proxy server, yang bertujuan untuk meminimalisir kerusakan yang disebabkan oleh serangan SYN Flood.
- Dampak dari serangan SYN FLOOD dapat dimitigasi dengan menggunakan “SYN cookie” pada perangkat firewall. Jika SYN cookie digunakan, firewall akan melakukan pemeriksaan koneksi TCP antara client dengan server sebelum traffic dikirim ke server. Jika penyerang tidak mengirimkan pesan ACK terakhir untuk koneksi tersebut, maka firewall akan langsung menutupnya.

UDP Flood Attack

User Datagram Protocol (UDP) Flood sangat mirip dengan SYN Flood. Penyerang mengirim traffic dalam jumlah besar ke server korban menggunakna botnet. Perbedaan UDP Flood dengan TCP Flood terdapat pada kecepatannya. UDP Flood dapat diproses lebih cepat, selain itu UDP Flood juga dapat mengkonsumsi semua bandwidth yang tersedia di jaringan, dibandingkan harus mengkonsumsi kapasitas server. Hal ini dapat menutup akses bagi pengguna lain secara langsung.

Serangan UDP Flood dapat terjadi karena sebuah program yang sedang berjalan terus menunggu saat-saat paket data diterima ketika server membuka port UDP. Ketika tidak ada paket yang diterima pada port tersebut, server akan mengirimkan balasan/respon kepada pengirim paket UDP melalui paket ICMP Destination Unreachable. Saat serangan dilakukan, paket UDP dikirim dalam jumlah besar sehingga semua bandwidth yang tersedia digunakan untuk mengirim balasan/respon.



Gambar 2.2. Gambaran UDP Flood Attack

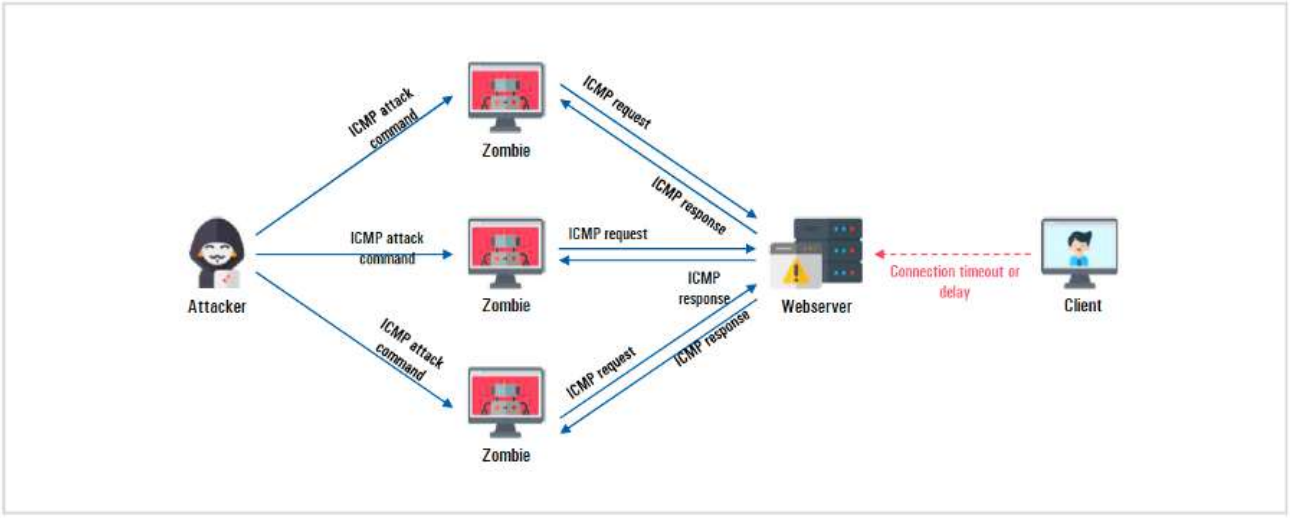
Tindakan Penanggulangan

- Carilah paket UDP yang menyerang dengan cara memeriksa log pada jaringan untuk melihat apakah terjadi UDP Flood. Periksa communication request dari port jaringan mencurigakan yang diterima dari berbagai sumber alamat IP.
- Beberapa layanan internet yang normal menggunakan UDP. Pada umumnya port UDP termasuk 53 (DNS), 88 (Kerberos), 137/138/445 (Windows), dan 161 (SNMP).
- Jika terdeteksi adanya sebuah serangan, mintalah tindakan penanggulangan kepada penyedia layanan jaringan (IPS, dll.) untuk melakukan mitigasi atas serangan tersebut.
- Untuk meminimalisir kerusakan yang disebabkan UDP Flood, buatlah rules untuk perangkat jaringan yang dibutuhkan, hal ini akan membatasi traffic untuk beberapa port yang diperlukan saja.

ICMP Flood Attack

Serangan ICMP (Internet Control Message Protocol) Flood terjadi ketika penyerang menggunakan botnet untuk mengirim paket ICMP dalam jumlah besar ke server target dengan tujuan untuk mengkonsumsi semua bandwidth yang tersedia dan mengganggu akses dari pengguna normal (normal users).

Serangan ini membutuhkan jumlah traffic permintaan (*request*) dan balasan (*response*) ICMP yang cukup untuk mengkonsumsi semua bandwidth yang tersedia pada jaringan target. Salah satu contoh serangan ini adalah perintah “ping”, yang biasanya digunakan untuk menguji koneksi antara dua titik dalam sebuah jaringan. Bagaimanapun, ukuran “ping” dan pengulangan request dapat diatur menggunakan perintah (command) dan parameter, yang mana dapat digunakan untuk menghabiskan seluruh bandwidth jaringan yang tersedia.



Gambar 2.3. Gambaran ICMP Flood Attack

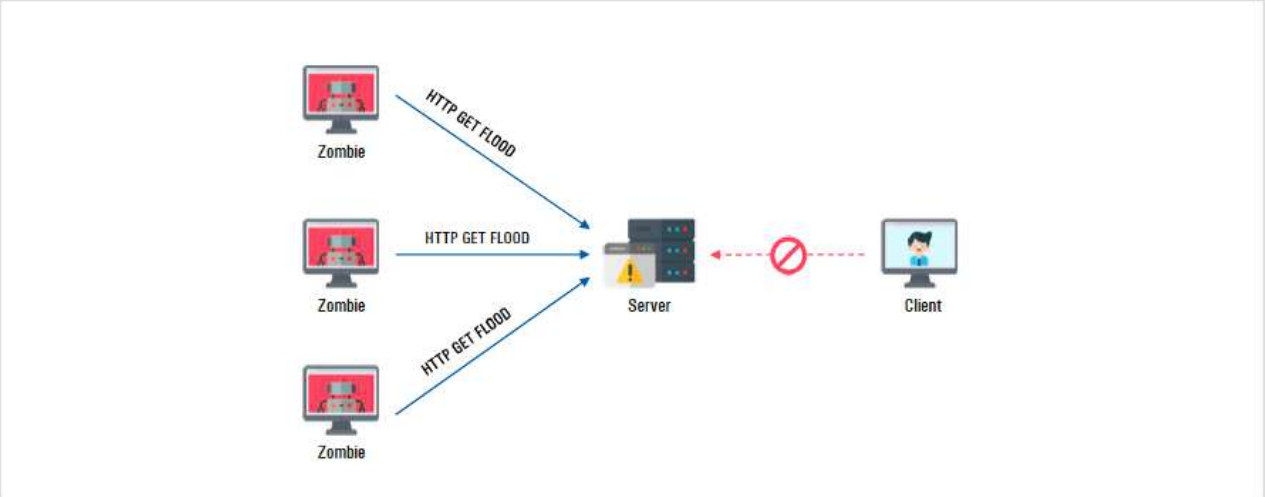
Tindakan Penanggulangan

- Periksa paket ICMP yang masuk dari permintaan/request pengguna di dalam log jaringan untuk melihat adanya ICMP Flood.
  - ICMP dapat diperiksa tergantung pada alat yang digunakan (misalnya Wireshark). ICMP tidak menggunakan port jaringan seperti TCP dan UDP.
  - Protokol ICMP dapat diidentifikasi dengan nomor protocol transport, "1", di header paket.
- Jika terdeteksi adanya sebuah serangan, mintalah tindakan penanggulangan kepada penyedia layanan jaringan (IPS, dll) untuk melakukan mitigasi atas serangan tersebut.
- Buatlah sebuah tahapan tambahan pada perangkat jaringan, seperti router, untuk meminimalisir kerusakan yang diakibatkan oleh ICMP Flood. Aturlah jumlah paket yang diperbolehkan melalui tahapan tersebut (per-detik) pada ICMP request di router-router lainnya. Ketika tahapan tambahan ini telah diatur, paket ICMP yang masuk akan ditolak untuk beberapa saat jika pada tahapan tambahan tersebut sudah melampaui batas jumlah. Tahapan ini bertujuan untuk mencegah jaringan bekerja berlebihan karena paket ICMP yang masuk.

HTTP Flood Attack

Hyper Text Transfer Protocol (HTTP) Flood membuat pengguna normal (normal user) tidak dapat menggunakan sumberdaya pada web server dengan mengirim HTTP GET request messages dalam jumlah besar kepada website yang ditargetkan. Dalam kasus ini, web server mencoba untuk merespon pada request si penyerang, namun penyerang tidak memproses acknowledgement (ACK) dan membuat web server menunggu. Alhasil, web server memproses koneksi ini dengan mengalokasikan sumberdaya selama jangka waktu tertentu untuk memeriksa acknowledgement.

Penyerang mengirim banyak HTTP GET request ke web server dan tidak memberikan acknowledgement sehingga web server yang diserang menggunakan semua sumberdaya komunikasi. Hal ini berakibat pengguna normal tidak dapat mengakses layanan website.



Gambar 2.4. Gambaran HTTP Flood Attack

Tindakan Penanggulangan

- Periksa jumlah request dalam jumlah banyak yang masuk ke port 80 dan protocol TCP pada log jaringan, untuk melihat apakah terjadi HTTP GET Flood.
- Direkomendasikan untuk menggunakan TCPdump dan Wireshark sebagai alat untuk memeriksanya.
- Jika terdeteksi adanya serangan, hubungi bagian dari perusahaan yang melayani perlindungan terhadap serangan DDoS.
- Memblokir seluruh sumber alamat IP sangatlah tidak efisien karena alamat IP pengguna normal bisa saja termasuk ke dalamnya. Apalagi mengingat alamat IP yang menjadi sumber serangan merupakan botnet.
- Kerusakan yang diakibatkan oleh serangan ini dapat diminimalisir dengan menggunakan *web application firewall* (WAF).

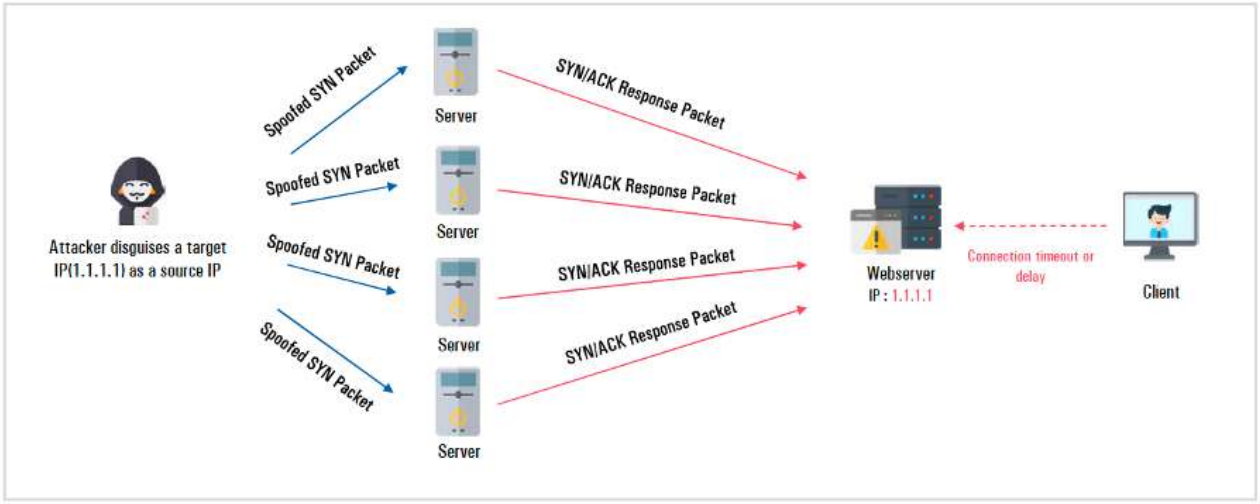
BAGIAN 3:

Jenis-Jenis Serangan *Reflection DDoS*

SYN + ACK Reflection Attack

SYN+ACK Flood adalah jenis serangan dengan metode Distributed Reflection Denial of Service (DRDoS). Penyerang mencuri IP korban dan mengirimkan paket SYN ke server untuk dieksploitasi sebagai reflektor, dan membuat server mengirim paket SYN/ACK ke komputer korban sebagai acknowledgment. Ketika komputer korban menerima paket SYN/ACK dalam jumlah besar, korban harus mengkonsumsi semua sumber daya yang ia punya untuk memporoses paket tersebut. Hal ini akan mengakibatkan server kewalahan dalam memprosesnya, sehingga akan mencegah pengguna normal untuk mengakses sumber daya.

Dikarenakan merupakan DRDoS, server reflector akan mengurim paket kembali jika entitas lain (korban) tidak melakukan acknowledge karena menganggapnya sebagai kegagalan transfer. Hal inilah meningkatkan efektifitas serangan SYN+ACK Reflection Attack.



Gambar 3.1.Gambaran SYN + ACK Reflection Attack

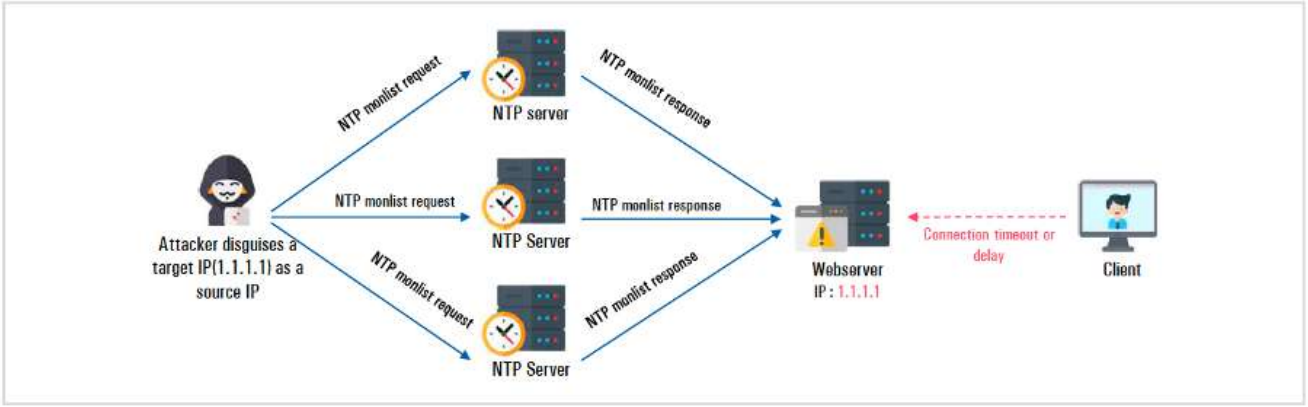
Tindakan Penanggulangan

- Periksa log pada jaringan dan cari TCP ACK flags untuk memeriksa adanya SYN/ACK Flood.
- Packet Analysis Tools seperti TCPdump atau Wireshark dapat digunakan.
- Paket TCP SYN/ACK diterima pada proses handshaking dalam 3 cara. Paket tersebut merupakan paket normal, tapi dapat dianggap sebagai serangan DDoS jika jumlah paket bertambah banyak dengan cepat dalam periode waktu yang singkat.
- Jika terdeteksi adanya sebuah serangan, mintalah penyedia layanan jaringan (IPS, dll.) untuk melakukan tindakan penanggulangan terhadap serangan.
- Atur filter paket SYN/ACK berdasarkan IP tujuan pada semua perangkat penting yang terhubung, seperti pada firewall dan proxy server untuk meminimalisir kerusakan yang diakibatkan oleh SYN/ACK Flood.

NTP Reflection & Amplification Attack

Serangan refleksi pada Network Time Protocol (NTP) adalah jenis serangan di mana si penyerang membuat lalulintas data pada server yang normal. NTP digunakan untuk mengsinkronisasi waktu pada server dan client, antara server dan server, serta menggunakan UDP port 123. Penyerang mencuri alamat IP target dan melakukan request ke server NTP untuk mengirim paket respon dengan ukuran tetap, dan dalam jumlah besar, kepada server yang ditargetkan.

Efisiensi serangan ini dapat ditingkatkan secara signifikan dengan menggunakan teknologi amplifikasi, yang memungkinkan server NTP merespon jumlah yang lebih besar terhadap reguest yang dikirim oleh si penyerang. Ketika ia mengirim request terhadap beberapa server NTP yang terbuka di internet, semua server tersebut akan mengirimkan respon mereka terhadap request tersebut secara bersamaan. Semua server target akan menggunakan seluruh bandwidth yang tersedia dan tidak dapat menyediakannya untuk pengguna normal (normal user).



Gambar 3.2. Gambaran NTP Reflection Attack

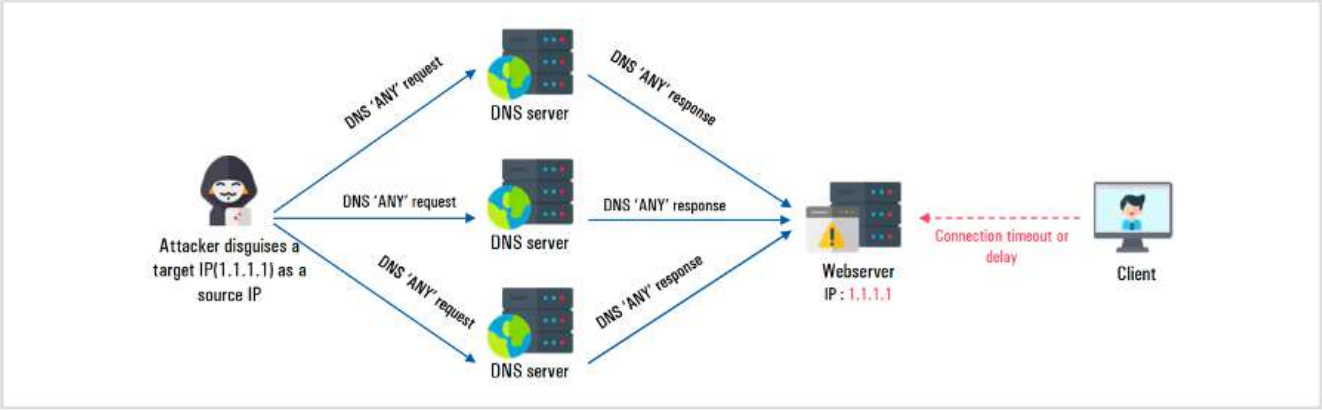
Tindakan Penanggulangan

- Periksa paket dengan port UDP 123 dan paket dengan ukuran tertentu pada semua sumber di network log in untuk mendeteksi adanya serangan refleksi dan aplifikasi NTP.
- Jika terdeteksi adanya serangan yang terjadi, sediakan informasi yang digunakan untuk serangan (alamat IP, ukuran paket, dll) kepada penyedia layanan jaringan (ISP, dll.) dan mintalah untuk dilakukan filter atau pembatasan.
- Ikuti langkah pencegahan berikut untuk melawan serangan yang masuk dan untuk mencegah server NTP dijadikan alat untuk menyerang pengguna lain:
  - Upgrade server NTP ke vesi 2.4.7 atau yang lebih baru untuk menghapus monlist command, atau gunakan versi NTP yang tidak menggunakan monlist command, seperti OpenNTPD.
  - Jika server tidak dapat di-upgrade, tambahkan “disable monitor” pada file ntp.conf kemudian restart proses NTP untuk menonaktifkan fungsi query.
  - Terapkan rules firewall yang dapat menolak paket tidak dikenal yang masuk ke server NTP

DNS Reflection & Amplification Attack

Pada serangan refleksi Domain Name Server (DNS), si penyerang mengeksploitasi sistem DNS untuk mengirim pesan dalam jumlah yang besar. Sistem DNS mengkonversi alamat domain (berbasis karakter) yang dimasuki oleh pengguna internet pada umumnya menjadi sebuah alamat IP. Serangan refleksi DNS menggunakan sebuah prosedur di mana si penyerang mencuri alamat IP milik korban dan mengirimkan respon kepada request si korban.

Jumlah respon pada saat itu tergantung pada pilihan yang disediakan oleh si penyerang pada DNS lookup request. Si penyerang dapat mendeskripsikan “ANY” untuk jumlah maksimal request yang masuk untuk memaksimalkann efek amplifikasinya.



Gambar 3.3. Gambaran DNS Reflection Attack

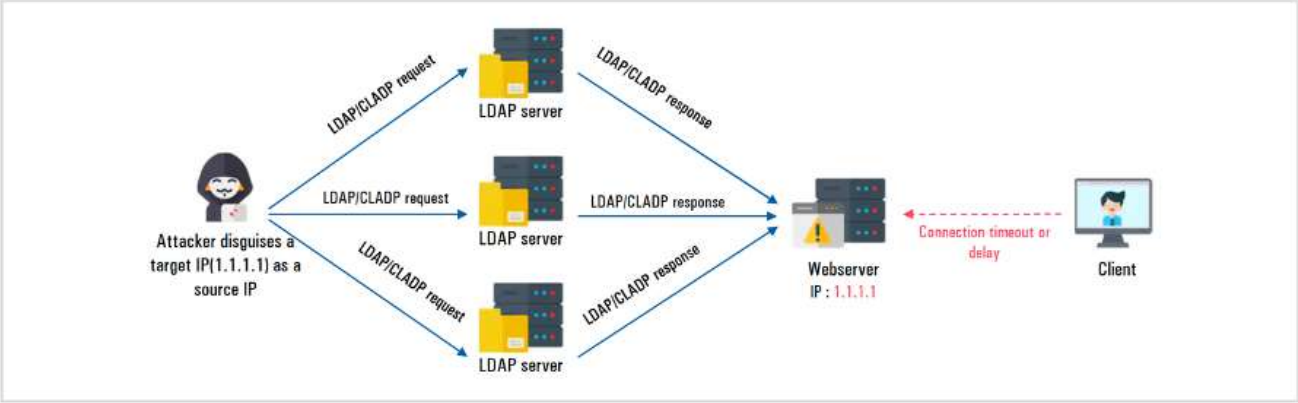
Tindakan Penanggulangan

- Periksa respon pada DNS query yang masuh tanpa adanya request DNS query pada network log dengan tujuan untuk mendeteksi adanya serangan refleksi dan aplifikasi DNS.
- Jika terdeteksi adanya serangan, hubungi penyedia layanan jaringan (ISP, dll.) untuk meminta agar paket serangan disaring sebelum dikirim ke server.
- Berdasarkan instruksi yang disediakan oleh pengembang DNS (seperti BIND, Microsoft, dll.), layanan DNS seharusnya tidak menggunakan fungsi pengulangan.
- Lakukan pengecekan tentang adanya eksploitasi terhadap DNS melelui website seperti: opensolverproject.org.

CLDAP Reflection & Amplification Attack

Pada serangan refleksi Connection-less Lightweight Dorectory Access Protocol (CLDAP), si penyerang mencuri alamat IP korban dan mengirim request CLDAP ke server LDAP.

CLDAP digunakan untuk membuat, mencari, dan memodifikasi direktori internet yang dibagikan, dan menggunakan port UDP 389. Serangan refleksi CLDAP terlihat ketika si penyerang mengirim CLDAP query ke berbagai server LDAP dengan menggunakan alamat IP yang dicuri tadi. Server LDAP akan mengirimkan respon berupa data kepada request alamat IP tersebut. Si korban tidak dapat menyediakan layanan normal karena sumber daya yang dimiliki tidak bisa menangani lalu lintas LDAP/CLDAP dalam jumlah besar yang masuk secara bersamaan. Protokol UDP LDAP akan meningkatkan efisiensi serangan dengan menggunakan teknologi amplifikasi yang dapat memperkuat serangan dari 52 menjadi 70 kali.



Gambar 3.4. Gambaran CLDAP Reflection Attack

Tindakan Penanggulangan

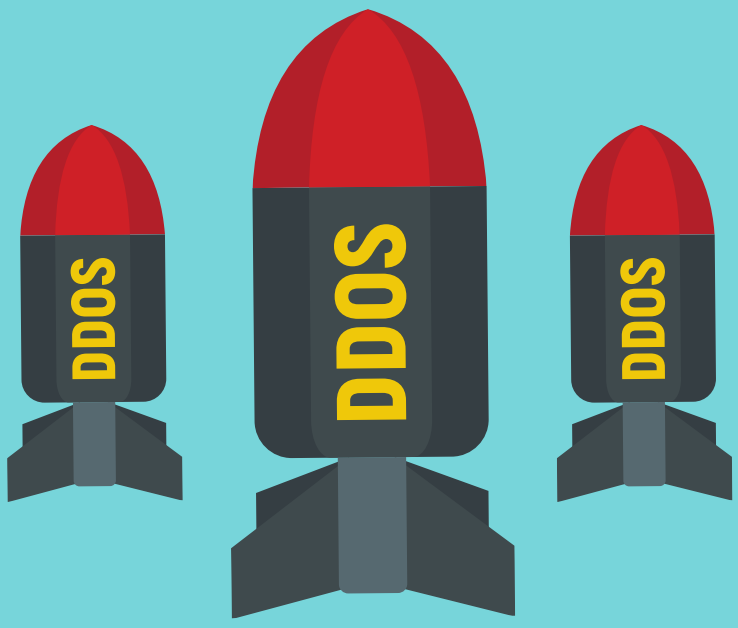
- Periksa log request yang menggunakan port UDP 389.
- Jika terdeteksi adanya serangan, hubungi penyedia layanan jaringan (ISP, dll.) untuk meminta agar paket-paket serangan disaring sebelum dikirim ke server.
- Ketika menjalankan server LDAP, gunakan rules firewall untuk mencegah adanya eksploitasi pada server LDAP.

BAGIAN 4:

Strategi Untuk Meminimalisir Kerusakan

Jika serangan DDoS terjadi, penting sekali bagi kita untuk mengaktifkan respon cepat (quick response) untuk meminimalisir kerusakan.

1. Memahami layanan pencegahan DDoS yang disediakan penyedia layanan jaringan (network service provider).
2. Pertimbangkan untuk memasukkan layanan pencegahan serangan DDoS dalam kontrak ketika anda membangun sebuah sistem dan jaringan.
3. Jika serangan DDoS terjadi, berikan alamat IP penyerang kepada penyedia layanan jaringan.
4. Periksa lokasi di mana serangan DDoS terjadi dengan memeriksa log firewall untuk melihat mana paket-paket yang diizinkan dan mana yang tidak diizinkan.
5. Cegah SYN Flood dengan melakukan setting “TCP keepalive” dan “Maximum Connections” pada perangkat-perangkat seperti firewall dan proxy server.
6. Periksa apakah penyedia layanan jaringan dapat melakukan penyaringan port dan ukuran paket, serta mengatur penyaringan (*filter*) jika mereka bisa.
7. Memahami pola paket normal (volume dan jenis) dari situs web publik, kemudian periksa apakah ada pola abnormal yang terjadi secara teratur.
8. Terapkan perbaikan (patch) pada jaringan maupun peralatan keamanan setelah melakukan pengujian dan verifikasi.
9. Konfigurasikan pengaturan firewall untuk memblokir lalu lintas masuk dari alamat IP yang di-*reserved* (0/8), loopback (127/8), privat (RFC 1918 block 10/8, 172.16/12 dan 192.168/16), client DHCP yang belum ditetapkan (169.254.0/16), multicast (224.0.0/4), dan alamat lain yang terdaftar di RFC 5735. Konfigurasi ini juga harus diminta kepada penyedia layanan jaringan untuk diterapkan.
10. Pahami proses serta jumlah bandwidth jaringan yang dibutuhkan untuk keperluan jalannya bisnis, kemudian periksa pengaturannya pada server.
11. Atur firewall sesuai dengan tujuan bisnis serta kebijakan keamanannya.
12. Konfigurasikan firewall dan intursion detection service (IDS) sebagai deteksi awal terhadap gejala abnormal pada jaringan.
13. Persiapkan cara alternatif pada koneksi untuk mengatasi kegagalan layanan jaringan dikarenakan serangan DDoS.
14. Pertimbangkan untuk menggunakan layanan respon terhadap serangan DDoS yang disediakan oleh pemerintah.



PUSAT OPERASI KEAMANAN SIBER NASIONAL

Ministry of Science and ICT

KISA KOREA INTERNET & SECURITY AGENCY

Pusopskamsinas
Badan Siber dan Sandi Negara
Republik Indonesia