5 Kasus Nyata Serangan Terhadap Jaringan Komputer

Nama: Rifqi Fadil Fahrial
NIM: 1222646

Kasus 1: Serangan WannaCry Ransomware (2017)

Latar Belakang: WannaCry adalah salah satu ransomware paling terkenal yang menyerang lebih dari 200.000 komputer di 150 negara. Serangan ini terjadi pada Mei 2017 dan memengaruhi berbagai organisasi, termasuk rumah sakit NHS di Inggris.

Bagaimana Serangan Terjadi:

- **Exploitasi Kerentanan EternalBlue:** WannaCry memanfaatkan kerentanan SMBv1 (Server Message Block version 1) yang dikenal sebagai EternalBlue. Kerentanan ini awalnya dikembangkan oleh NSA dan kemudian bocor oleh kelompok peretas Shadow Brokers.
- **Eksekusi Payload:** Setelah berhasil mengeksploitasi kerentanan, WannaCry mengunduh payload ransomware dari server penyerang. Payload ini berisi algoritma enkripsi AES-128 untuk mengunci file pengguna.
- **Penyebaran Otomatis:** WannaCry menggunakan modul worm-like bernama DoublePulsar untuk menyebar ke komputer lain dalam jaringan tanpa intervensi manusia. Worm ini mencari komputer yang rentan melalui port TCP 445.
- **Permintaan Tebusan:** Setelah file dienkripsi, ransomware menampilkan pesan tebusan yang meminta pembayaran dalam Bitcoin. Jika tebusan tidak dibayar dalam waktu tertentu, jumlah tebusan akan meningkat.

Kasus 2: Serangan DDoS pada DynDNS (2016)

Latar Belakang: Serangan Distributed Denial of Service (DDoS) terhadap DynDNS pada Oktober 2016 menyebabkan downtime besar-besaran pada banyak situs web populer seperti Twitter, Reddit, dan Netflix.

Bagaimana Serangan Terjadi:

- **Botnet Mirai:** Penyerang menggunakan botnet Mirai, yang terdiri dari ratusan ribu perangkat IoT (seperti kamera IP dan router) yang telah diinfeksi malware. Perangkat ini dikendalikan secara remote untuk meluncurkan serangan.

- **Teknik Amplifikasi DNS:** Botnet mengirimkan permintaan DNS yang sengaja dibuat besar ke server DynDNS. Permintaan ini memicu respons DNS yang jauh lebih besar, sehingga memperbesar volume lalu lintas serangan.
- **Overload Server:** Volume lalu lintas yang sangat besar menyebabkan server DynDNS tidak dapat merespons permintaan DNS dari pengguna, mengakibatkan downtime pada banyak situs web yang bergantung pada layanan DynDNS.
- **Efek Domino:** Karena DynDNS adalah penyedia DNS utama untuk banyak situs web, serangan ini menyebabkan gangguan global pada layanan internet.

Kasus 3: Serangan SQL Injection pada Equifax (2017)

Latar Belakang: Serangan SQL injection pada Equifax pada Juli 2017 mengakibatkan pencurian data pribadi lebih dari 147 juta orang. Ini adalah salah satu pelanggaran data terbesar dalam sejarah.

Bagaimana Serangan Terjadi:

- **Vulnerabilitas Apache Struts:** Penyerang mengeksploitasi kerentanan dalam framework Apache Struts (CVE-2017-5638) yang digunakan oleh aplikasi web Equifax. Kerentanan ini memungkinkan eksekusi kode jarak jauh.
- **Injeksi SQL:** Melalui input yang dimanipulasi, penyerang dapat menyuntikkan perintah SQL ke dalam query database. Ini memungkinkan mereka mengakses dan mengekstrak data sensitif.
- **Data Exfiltration:** Setelah mendapatkan akses ke database, penyerang mengunduh data pribadi pelanggan, termasuk nomor Jaminan Sosial, nomor SIM, alamat, dan informasi kartu kredit.
- **Kelemahan Keamanan:** Equifax gagal memperbarui patch keamanan untuk kerentanan Apache Struts, meskipun patch sudah tersedia selama beberapa bulan sebelum serangan.

Kasus 4: Serangan Phishing pada Target Corporation (2013)

Latar Belakang: Serangan phishing pada Target Corporation pada akhir 2013 mengakibatkan pencurian data kartu kredit lebih dari 40 juta pelanggan.

Bagaimana Serangan Terjadi:

- **Email Phishing:** Penyerang mengirim email palsu kepada karyawan vendor HVAC yang bekerja dengan Target. Email tersebut berisi lampiran malware yang tampaknya berasal dari vendor tepercaya.
- **Infeksi Malware:** Setelah karyawan mengklik lampiran, malware diinstal di komputer mereka. Malware ini memberikan akses jarak jauh ke jaringan internal Target.

- **Akses ke Jaringan POS:** Penyerang menggunakan akses ini untuk menyusup ke sistem Point of Sale (POS) Target. Mereka menginstal malware POS yang mencuri data kartu kredit dari transaksi pelanggan.
- **Exfiltrasi Data:** Data kartu kredit yang dicuri dikirimkan ke server penyerang melalui jaringan Target. Proses ini berlangsung selama beberapa minggu tanpa terdeteksi.

Kasus 5: Serangan Cryptojacking pada Tesla (2018)

Latar Belakang: Serangan cryptojacking pada Tesla terjadi pada Februari 2018. Penyerang berhasil menyusup ke cluster Kubernetes milik Tesla dan menggunakan sumber daya komputasi untuk menambang cryptocurrency Monero.

Bagaimana Serangan Terjadi:

- **Kerentanan Kubernetes:** Penyerang menemukan cluster Kubernetes Tesla yang tidak dilindungi kata sandi atau autentikasi lainnya. Cluster ini digunakan untuk menjalankan container aplikasi.
- **Penyisipan Script Penambangan:** Setelah mendapatkan akses, penyerang menyisipkan script penambangan cryptocurrency (cryptojacking) ke dalam container yang berjalan.
- **Penambangan Cryptocurrency:** Script ini menggunakan sumber daya CPU dan GPU Tesla untuk menambang Monero, cryptocurrency yang dirancang untuk anonimitas.
- **Penggunaan Sumber Daya:** Aktivitas penambangan ini menguras sumber daya komputasi Tesla tanpa izin, menghasilkan biaya tambahan dan potensi gangguan pada operasi normal.
- **Deteksi Lambat:** Serangan ini hanya terdeteksi setelah RedLock Cloud Security Intelligence melaporkannya kepada Tesla.