*Nama : Muhammad Yusril* Nis. *11907393*

*Rombel. : RPL XI 3* Rayon. : Cisarua 01

*Resume Cyber security Minggu ke 7*

*Networking Protocols and Threats*

*Seperti halnya retakan di bendungan kerentanan terhadap apa pun yang berdiri di lembah* terdekat, port terbuka juga rentan terhadap jaringan komputer. Serangan flooding (membanjiri) jaringan tampaknya tak ada habisnya; dan meskipun serangan jaringan baru terus-menerus dirancang, ancaman ini harus ditangani secara proaktif.

*Selain semua metafora, ini berarti Anda harus memiliki pemahaman menyeluruh tentang banyak* protokol jaringan yang digunakan saat ini, dan nomor port yang sesuai. Pengetahuan tentang port masuk adalah yang paling penting karena berkorelasi dengan layanan yang berjalan di server; ini adalah pintu yang digunakan penyerang untuk mengakses sistem. Server yang menjalankan protokol seperti HTTP, FTP, SMTP, dan sebagainya harus diperbarui, di hardening, dan diamankan dengan tepat. Versi aman dari protokol ini harus diimplementasikan. Protokol dan layanan yang tidak penting (seperti Telnet yang sudah usang atau, misalnya, TFTP) harus dihentikan dan dinonaktifkan. Ini secara efektif menutup port yang dimaksud. Anda harus mengingat port yang disebutkan dalam bab ini karena Anda akan memindai port terbuka seperti ini di bab-bab berikutnya. Jika ada kebingungan tentang port atau protokol, ingatlah untuk mengakses situs web IANA untuk informasi lebih lanjut.

*Inti dari mengurangi permukaan serangan suatu sistem adalah agar serangan jahat lebih sulit* mengakses sistem itu. Sebagai contoh, katakanlah Anda memiliki server yang menjalankan Layanan Informasi Internet Microsoft (IIS) dan memiliki situs web yang menjalankannya yang menggunakan HTTP, tetapi Anda secara tidak sadar juga menjalankan FTP di server itu, menggunakan port 21. Server bisa menjadi mangsa yang mudah untuk serangan yang dirancang untuk menyusup melalui port 21. Tetapi tidak harus seperti ini! Menggunakan port aman, menutup port, menonaktifkan layanan, dan, tentu saja, menggunakan firewall adalah pertahanan vital. Bab 8 mencakup peralatan tambahan seperti sistem deteksi intrusi jaringan, proksi, dan berbagai jenis firewall.

*Di zaman sekarang ini ada banyak sekali serangan jaringan. Saat mengamati jaringan dan* server Anda, serangan seperti penolakan layanan (DoS), DoS yang didistribusikan (DDoS), spoofing, pembajakan, replay, amplifikasi, dan keracunan harus berada di bagian atas daftar Anda. Selain sebagai penyelidik, salah satu peran Anda adalah sebagai peneliti. Anda harus

*mempelajari serangan terbaru dan CVE untuk suatu sistem, mengawasi pembaruan dan buletin,* dan sering mengunjungi forum online dan grup diskusi. Namun, peran "pengamat" mungkin adalah salah satu istilah deskriptif terbaik untuk administrator keamanan. Anda harus terus- menerus memeriksa server dan peralatan jaringan Anda. Penjagaan abadi ini adalah bagian dari pekerjaan. Mereka yang waspada dan jeli akan menang, dan mereka yang tidak baik, mereka berisiko dibanjiri dengan ancaman yang bersembunyi di luar (dan kadang-kadang di dalam) jaringan komputer.