Nama: Kristian Binsar Pardamean Pasaribu
Nim: 2702278625

CATATAN MATERI SESI 12: OPERATING SYSTEM SECURITY

1. Konsep Dasar Keamanan

Keamanan sistem berarti seluruh resource digunakan sesuai tujuan di semua kondisi. Serangan dapat bersifat tidak sengaja maupun berbahaya.

Istilah utama:

Threat adalah potensi pelanggaran. Attack adalah upaya nyata untuk melanggar keamanan.

Kategori pelanggaran:

Breach of confidentiality, integrity, availability, theft of service, dan denial of service.

Metode serangan:

Masquerading, replay attack, man-in-the-middle, session hijacking, privilege escalation.

2. Level-Level Keamanan

Efektivitas keamanan bergantung pada empat level:

Physical (keamanan perangkat), *Application* (keamanan software), *Operating System* (proteksi & kontrol), dan *Network* (serangan komunikasi).

Titik terlemah menentukan keseluruhan keamanan, termasuk faktor manusia.

3. Program Threats

Malware meliputi virus, worm, trojan horse, spyware, ransomware.

Trapdoor/backdoor adalah jalur masuk tersembunyi di dalam program.

Logic bomb aktif jika kondisi tertentu terpenuhi.

4. Code Injection & Buffer Overflow

Code injection terjadi ketika data berbahaya disisipkan ke dalam program akibat kurangnya validasi input.

Buffer overflow muncul saat input melebihi kapasitas buffer hingga menimpa memori lain seperti return address.

Eksploitasi membutuhkan pemahaman struktur memori proses untuk mengarahkan flow eksekusi.

Tujuan umum: menjalankan kode penyerang, membuka shell, atau merusak proses.

5. Ancaman Sistem & Jaringan

Worm: menyebar otomatis melalui jaringan, memanfaatkan celah layanan seperti sendmail atau trust relationship.

Port Scanning: pemindaian port untuk menemukan layanan aktif.

DoS dan DDoS: membanjiri target sehingga layanan tidak tersedia.

6. Authentication

Autentikasi adalah proses memastikan identitas user.

Tahapan:

identification (menyatakan identitas) dan *verification* (membuktikan identitas).

7. Pertahanan Keamanan

Defense in Depth: pendekatan berlapis untuk meminimalkan risiko.

Mekanisme pertahanan meliputi *signature detection*, *anomaly detection*, *sandboxing*, *virus scanning*, *auditing*, *logging*.

Tujuannya mendeteksi pola berbahaya atau perilaku tidak normal, termasuk zero-day attack.

8. Firewall

Firewall memisahkan jaringan trusted dan untrusted.

Bentuknya meliputi *network firewall*, *personal firewall*, *application proxy*, dan *system-call firewall*.

Dapat dilewati dengan tunneling atau spoofing jika konfigurasi lemah.

9. Countermeasures terhadap Buffer Overflow

Compile-Time Defenses: Language extensions yang menambah pengecekan batas, safe libraries (misalnya Libsafe), stack protection seperti StackGuard, pemilihan bahasa pemrograman aman, dan audit kode.

Runtime Defenses: Guard pages sebagai area ilegal, non-executable memory melalui NX-bit, serta ASLR yang mengacak lokasi memori untuk mempersulit prediksi alamat.

10. Access Control

Access control mengatur siapa bisa melakukan apa terhadap resource.

Jenis hak akses: none, knowledge, execution, reading, appending, updating, changing protection, deletion.

Kebijakan kontrol akses:

Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role-Based Access Control (RBAC), dan Attribute-Based Access Control (ABAC).

UNIX menggunakan permission (r w x) untuk owner, group, dan others.

11. OS Hardening

Langkah utama memperkuat OS:

1. Instal & patch OS secara berkala.
2. Hapus service, aplikasi, dan protokol yang tidak diperlukan.
3. Konfigurasi user, group, permission, dan password policy.
4. Atur resource control agar akses sesuai kebutuhan.
5. Tambahkan antivirus, firewall, IDS/IPS jika diperlukan.
6. Uji keamanan untuk memastikan konfigurasi benar.

12. Security Maintenance

Meliputi *logging*, *rotasi log*, *analisis otomatis*, *backup berkala*, dan *archive jangka panjang* untuk kebutuhan operasional maupun legal.

Audit keamanan harus dilakukan secara periodik.

13. Windows Access Control

Saat user login, sistem membuat access token yang berisi SID user dan SID group. Token ini digunakan untuk menentukan hak akses setiap proses yang dijalankan user.