Panduan Final Project

Matakuliah: Perancangan Keamanan Sistem dan Jaringan

A. Panduan Umum

1. Setiap mahasiswa tergabung dalam sebuah kelompok Final Project.
2. Kelompok berisikan anggota 5-6 orang
3. Membuat Laporan Akhir Final Project.
4. Setiap kelompok mengerjakan Final Project sesuai studi kasus yang ditetapkan.
5. Mengunggah source code final project pada laman Github. (Github harus dapat diakses oleh public).
6. Melakukan presentasi akhir final project.
7. Pengisian link anggota kelompok dilakukan pada link yang ditentukan.

B. Studi Kasus

Studi Kasus 1: Implementasi Firewall dan Analisis Keamanannya

Rumusan Masalah: Bagaimana konfigurasi firewall yang efektif dapat melindungi sistem dari ancaman eksternal dan internal?

Langkah-langkah:

Minggu 1: Pelajari dasar-dasar firewall dan pilih perangkat lunak/hardware firewall (contoh: pfSense).
Minggu 2: Pasang dan konfigurasikan firewall di lingkungan virtual atau fisik.
Minggu 3: Uji aturan dasar untuk memblokir port dan alamat IP tertentu.
Minggu 4: Simulasikan serangan seperti port scanning dan analisis log.
Minggu 5: Dokumentasikan hasil pengujian dan analisis efektivitas firewall.

Studi Kasus 2: Membangun IDS/IPS Berbasis Open Source

Rumusan Masalah: Seberapa efektif IDS/IPS berbasis open source (contoh: Snort atau Suricata) dalam mendeteksi ancaman jaringan?
Langkah-langkah:
Minggu 1: Instal dan pelajari dasar-dasar IDS/IPS pilihan Anda.
Minggu 2: Konfigurasikan aturan deteksi ancaman umum seperti port scanning atau brute force.
Minggu 3: Simulasikan ancaman menggunakan alat seperti Metasploit atau hping3.
Minggu 4: Analisis log IDS/IPS untuk mendeteksi dan mencegah ancaman.
Minggu 5: Evaluasi efektivitas sistem dan usulkan perbaikan.

Studi Kasus 3: Mengamankan Aplikasi Web dari Serangan DDoS

Rumusan Masalah: Bagaimana strategi proteksi berbasis cloud dapat melindungi aplikasi web dari serangan DDoS?
Langkah-langkah:

Minggu 1: Buat aplikasi web sederhana dan host di platform cloud.
Minggu 2: Implementasikan layanan seperti AWS Shield atau Cloudflare.
Minggu 3: Simulasikan serangan DDoS menggunakan alat seperti LOIC.
Minggu 4: Analisis respons aplikasi dan dokumentasikan log serangan.
Minggu 5: Evaluasi keberhasilan strategi pertahanan yang diterapkan.

Studi Kasus 4: Enkripsi End-to-End pada Aplikasi Pesan

Rumusan Masalah: Bagaimana implementasi algoritma RSA dapat menjamin privasi komunikasi di aplikasi pesan?
Langkah-langkah:
Minggu 1: Buat aplikasi pesan sederhana menggunakan Python/Java.
Minggu 2: Tambahkan fitur enkripsi menggunakan algoritma RSA untuk pesan.
Minggu 3: Implementasikan pembagian kunci publik dan pribadi antar pengguna.
Minggu 4: Uji keamanan komunikasi dengan simulasi intercept pesan.
Minggu 5: Dokumentasikan hasil implementasi dan evaluasi kinerja.

Studi Kasus 5: Membangun Honeypot untuk Deteksi Ancaman

Rumusan Masalah: Apa jenis ancaman yang paling umum dideteksi oleh honeypot di jaringan lokal?
Langkah-langkah:
Minggu 1: Pelajari dasar-dasar honeypot dan pilih alat seperti Cowrie atau Dionaea.
Minggu 2: Instal dan konfigurasikan honeypot di lingkungan jaringan lokal.
Minggu 3: Jalankan honeypot selama beberapa hari untuk mengumpulkan data serangan.
Minggu 4: Analisis log dan identifikasi pola serangan.
Minggu 5: Dokumentasikan hasil analisis dan usulkan langkah mitigasi ancaman.

Studi Kasus 6: Mengintegrasikan DNSSEC untuk Keamanan DNS

Rumusan Masalah: Bagaimana DNSSEC dapat melindungi sistem dari serangan DNS spoofing atau cache poisoning?
Langkah-langkah:
Minggu 1: Pelajari konsep DNS dan DNSSEC.
Minggu 2: Siapkan server DNS dan aktifkan DNSSEC.
Minggu 3: Buat zona DNS dengan tanda tangan digital menggunakan DNSSEC.
Minggu 4: Simulasikan serangan DNS spoofing dan analisis respons server.
Minggu 5: Evaluasi efektivitas DNSSEC dan dokumentasikan temuan.

Studi Kasus 7: Deteksi Malware di Jaringan Menggunakan Machine Learning

Rumusan Masalah: Bagaimana model machine learning dapat digunakan untuk mendeteksi malware dalam lalu lintas jaringan?
Langkah-langkah:
Minggu 1: Kumpulkan dataset lalu lintas jaringan (benign dan malicious).
Minggu 2: Pra-proses data dan pilih algoritma ML (contoh: Random Forest atau SVM).
Minggu 3: Latih model dengan dataset dan evaluasi akurasi model.

Minggu 4: Uji model dengan data baru dari lingkungan jaringan nyata.
Minggu 5: Analisis hasil dan sediakan rekomendasi peningkatan.

Studi Kasus 8: Mengamankan API dengan OAuth 2.0

Rumusan Masalah: Bagaimana OAuth 2.0 dapat diterapkan untuk melindungi API dari akses tidak sah?
Langkah-langkah:
Minggu 1: Buat API sederhana dengan autentikasi dasar.
Minggu 2: Implementasikan OAuth 2.0 untuk autentikasi dan otorisasi API.
Minggu 3: Simulasikan skenario serangan seperti token hijacking.
Minggu 4: Uji keamanan dengan alat pengujian API seperti Postman.
Minggu 5: Evaluasi penerapan OAuth 2.0 dan dokumentasikan proses.

Studi Kasus 9: Analisis Kerentanan Aplikasi Web dengan OWASP ZAP

Rumusan Masalah: Bagaimana OWASP ZAP dapat digunakan untuk mengidentifikasi kerentanan umum di aplikasi web?
Langkah-langkah:
Minggu 1: Pelajari dasar-dasar OWASP ZAP dan persiapkan aplikasi web target.
Minggu 2: Konfigurasikan OWASP ZAP untuk pemindaian aplikasi web.
Minggu 3: Lakukan analisis kerentanan seperti SQL injection atau XSS.
Minggu 4: Dokumentasikan hasil pemindaian dan sediakan rekomendasi mitigasi.
Minggu 5: Terapkan mitigasi dan uji ulang keamanan aplikasi.

Studi Kasus 10: Implementasi Zero Trust Architecture dalam Jaringan Perusahaan

Rumusan Masalah: Bagaimana pendekatan Zero Trust dapat meningkatkan keamanan jaringan perusahaan?
Langkah-langkah:
Minggu 1: Pelajari konsep Zero Trust dan identifikasi kebutuhan keamanan jaringan.
Minggu 2: Konfigurasikan autentikasi berbasis identitas (contoh: MFA).
Minggu 3: Implementasikan segmentasi jaringan berbasis perangkat atau pengguna.
Minggu 4: Uji skenario akses tidak sah dan validasi kontrol keamanan.
Minggu 5: Evaluasi efektivitas Zero Trust dan dokumentasikan hasil.

Kriteria Penilaian (Maks 100 poin)

1. **Pemahaman Materi/Teori (20 poin)**
    a. 0–5: Tidak memahami konsep dasar yang terkait dengan proyek.
    b. 6–10: Memahami sebagian konsep, tetapi terdapat kesalahan mendasar.
    c. 11–15: Memahami konsep dengan baik, beberapa bagian kurang mendalam.
    d. 16–20: Memahami teori dengan sangat baik dan mampu mengaitkannya dengan proyek.
2. **Implementasi Teknis (40 poin)**
    a. 0–10: Implementasi gagal dilakukan atau tidak sesuai spesifikasi.
    b. 11–20: Implementasi dasar dilakukan, tetapi terdapat banyak kesalahan.
    c. 21–30: Implementasi berfungsi sebagian dan menunjukkan pemahaman.

    d. 31–40: Implementasi sepenuhnya berfungsi sesuai spesifikasi dan efisien.
3. **Analisis dan Evaluasi (20 poin)**
    a. 0–5: Tidak ada evaluasi atau analisis terhadap hasil proyek.
    b. 6–10: Analisis dilakukan, tetapi kurang mendalam dan tidak relevan.
    c. 11–15: Analisis cukup mendalam, tetapi beberapa temuan kurang dijelaskan.
    d. 16–20: Analisis mendalam, relevan, dan menjelaskan temuan dengan jelas.
4. **Dokumentasi Laporan dan Presentasi (20 poin)**
    a. 0–5: Tidak ada dokumentasi atau presentasi, atau tidak relevan.
    b. 6–10: Dokumentasi dasar dengan banyak kekurangan.
    c. 11–15: Dokumentasi cukup lengkap, tetapi presentasi kurang menarik.
    d. 16–20: Dokumentasi sangat baik, terstruktur, dan presentasi menarik.

Format Laporan

Abstraksi
- Gambaran umum sistem (singkat)
- Tujuan pembuatan/desain sistem
- Hanya 1 paragraph (maks 250 kata)

#BAB 1. Pendahuluan
- Gambaran umum sistem yg dijelaskan secara detail
- Landasan pembuatan system beserta rumusan masalah yang diangkat
- Penjelasan tujuan desain sistem

#BAB 2. Literature review
- Penjelasan dasar teori yang digunakan
- Pembahasan sistem terdahulu yg sesuai dengan topik desain (referensi)

#BAB 3. Desain sistem
- Penjelasan teknologi yg mendukung sistem (arsitektur sistem)
- Penjelasan bagaimana desain sistem bekerja (Berisikan flowchart dan gambar rancangan system)

#BAB 4. Implementasi sistem
- Pembahasan implementasi system
- Tampilan dan penjelasan fitur-fitur aplikasi dari sistem
- Pengujian sistem

#BAB 5. Kesimpulan
- 1 Paragrap kesimpulan akhir dr desain sistem, dan menjawab rumusan masalah (Rumusan Masalah).

Referensi
- Daftar referensi yang digunakan

Jadwal Pengerjaan

1. Nov/25 - Nov/29 Progress Report 1
2. Des/2 - Des/6 Progress Report 2
3. Des /9 - Des /13 Progress Report 3
4. Des /16 - Des /20 Progress Report 4
5. Des /23 - Des /27 Progress Report 5
6. Jan/6 - Jan/10 Final Project Presentation and Demo