LAPORAN RESMI
KEMANAN JARINGAN

Cybersecurity Framework

Dosen :
Dr. Ferry Astika Saputra ST, M.Sc
Oleh :
Septiana Dyah Anissawati
D4 LJ Teknik Informatika B
3122640031

POLITEKNIK ELEKTRONIKA NEGERI SURABAYA
TAHUN AJARAN
2022/2023

Insinyur Jaringan

Insinyur Jaringan bertanggung jawab untuk mengimplementasikan, memelihara, mendukung, dan merancang jaringan komunikasi dalam sebuah organisasi atau antara organisasi.

Tujuannya adalah untuk memastikan ketersediaan tinggi dari infrastruktur jaringan untuk memberikan kinerja maksimum bagi penggunanya. Pengguna dapat berupa:

- Karyawan
- Klien
- Pelanggan
- Pemasok Eksternal

Peran Insinyur Jaringan:

- Mengkonfigurasi perangkat jaringan (seperti router, firewall, dan DS) dengan aman
- Menjamin sistem jaringan yang aman dengan menetapkan dan memantau kebijakan akses
- Mendukung dan mengelola lingkungan firewall sesuai dengan kebijakan keamanan IT
- Memahami masalah keamanan pada berbagai lapisan jaringan.

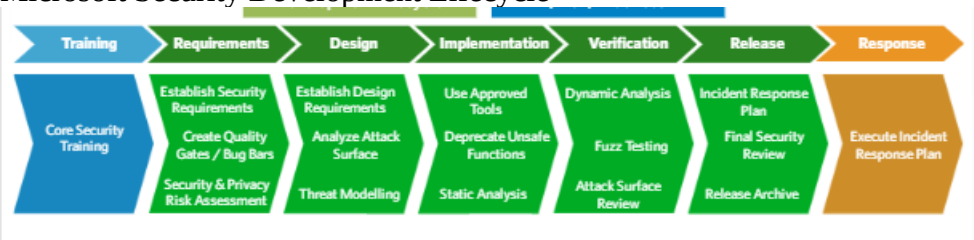
Pengembang Perangkat Lunak

Pengembang perangkat lunak bertanggung jawab untuk menulis dan mengkodekan program individual atau menyediakan sumber daya perangkat lunak baru secara keseluruhan berdasarkan kebutuhan.

Dari perspektif keamanan, ada kebutuhan untuk memahami atau menghargai area berikut.

- Berbagai jenis ancaman keamanan
- Praktik pemrograman yang aman sehingga program aman termasuk mengintegrasikan pustaka & kerangka kerja keamanan
- Menangani kerentanan yang ditemukan dan menyediakan patch
- Melakukan audit kode atau pengujian keamanan pada program atau aplikasi.

Microsoft Security Development Lifecycle



OWASP Secure Coding (Web) Practices

Analis Keamanan

Analis Keamanan bertanggung jawab untuk merencanakan dan menerapkan tindakan keamanan untuk melindungi sistem komputer, jaringan, dan data.

Mereka diharapkan untuk selalu mengetahui ancaman dan tren keamanan terbaru, termasuk teknik serangan, untuk mengantisipasi pelanggaran keamanan.

Tugas Tambahan Seorang Analis Keamanan:

- Mengembangkan kemampuan untuk mendeteksi ancaman dan pelanggaran kebijakan.

- Membuat, menguji dan menerapkan rencana pemulihan bencana
- Melakukan penilaian risiko dan kerentanan

Keterampilan yang dibutuhkan untuk Analis Keamanan:

- Pemahaman yang baik tentang jaringan, sistem operasi, dan kontrol keamanan
- Penyelesaian masalah
- Script

Analis Forensik Digital

Analis Forensik Digital memulihkan dan memeriksa data dari komputer dan perangkat penyimpanan elektronik lainnya untuk menggunakan bukti data dalam penyelidikan atau tuntutan pidana.

Pentingnya Analis Forensik Digital

Keahlian mereka penting dalam membantu memahami akibat dari serangan atau pelanggaran keamanan dunia maya. Ini terkadang membutuhkan informasi yang berhubungan yang diperoleh dari log, arus bersih, dan sumber daya lainnya.

Keterampilan yang diperlukan untuk Analis Forensik Digital:

- Pemahaman yang kuat tentang cara kerja Sistem Operasi (memori, sistem file, registri)
- Keakraban dengan alat-alat khusus

Auditor Keamanan

Auditor Keamanan bertanggung jawab untuk memastikan bahwa rencana dan kontrol keamanan diterapkan dengan benar.

Mereka membantu mengidentifikasi praktik yang tidak sesuai dengan kebijakan atau standar yang ada. Selain itu, mereka akan membahas peluang untuk perbaikan dengan pemangku kepentingan terkait.

Keterampilan yang dibutuhkan untuk Auditor Keamanan:

- Berpengalaman dalam standar keamanan
- Pemahaman teknis yang kuat tentang lingkungan yang diaudit
- Perhatian terhadap detail

Penguji Penetrasi

Penguji Penetrasi bertanggung jawab untuk menguji keamanan keseluruhan organisasi dengan mencari cara untuk mengeksploitasi kelemahan dalam jaringan, perangkat lunak, sistem, atau staf.

Mereka biasanya akan bekerja sama dengan pemangku kepentingan lain untuk memastikan bahwa kerentanan yang mereka temukan telah diperbaiki.

Berbagai jenis tes meliputi:

- Sistem internal atau eksternal (yaitu web, nirkabel)
- Berbagai jenis aplikasi
- Melakukan serangan rekayasa sosial
- Salah konfigurasi

Skill yang dibutuhkan untuk Penetration Tester :

- Pemahaman keamanan yang baik
- Latar belakang teknis yang kuat di berbagai bidang - termasuk jaringan, sistem operasi, protokol, dan pemrograman

Level eksekutif

Chief Executive Officer (CEO) dan manajemen puncak organisasi memiliki peran besar dalam implementasi keamanan secara keseluruhan.

Peran Tingkat Eksekutif

- Pastikan strategi keamanan tersedia, sumber daya yang cukup dialokasikan untuk keamanan, dan pahami kemampuan pertahanan dunia maya organisasi
- Tunjukkan kepemimpinan dengan contoh. Keamanan dunia maya adalah salah satu prioritas utama dan faktor penentu keberhasilan bagi organisasi.

Module 4 : Cyber Security Professionals

Which role is responsible for ensuring internally developed web applications are not vulnerable to attacks such as SQL injection or Cross-Site Scripting?

- (●) Software Developer
- ( ) Security Analyst
- ( ) Network Engineer
- ( ) Security Auditor

- **Software developers** are responsible for developing and maintaining the codebase for web applications, including ensuring that the code is secure and not vulnerable to common attack methods such as SQL injection or Cross-Site Scripting (XSS).
- **Security Analysts** are responsible for analyzing and identifying security threats to an organization's information systems and applications, and developing and implementing strategies to mitigate these threats.
- **Network Engineers** are responsible for designing, implementing, and maintaining an organization's network infrastructure.
- **Security Auditors** are responsible for evaluating an organization's security framework and ensuring it meets regulatory and industry standards.

So, the right answer is Software developer.

One of the responsibilities of a security auditor is to

- ( ) Configure firewall rules
- ( ) Write signatures for the intrusion detection system
- ( ) Analyze logs and netflows for signs of attacks
- (●) Ensure compliance to security policies

Security auditors may be responsible for evaluating an organization's security framework, identifying vulnerabilities and risks, and ensuring that the organization complies with relevant security policies, standards, and regulations. This could involve assessing security, evaluating security controls, and suggesting areas for improvement. The role of the security auditor may be to help ensure that the organization implements security policies and procedures effectively and that these policies are aligned with industry best practice and regulatory requirements.

Which of the following is ultimately responsible for formulating the security strategy and making sure that resources are allocated for the organization-wide security program?

- (●) Top Management
- ( ) Security Analyst
- ( ) Security Auditor
- ( ) Penetration Tester

Top management is responsible for defining the organization's security strategy and ensuring that it is aligned with business goals and objectives. This includes identifying key security risks, developing security policies and procedures, and allocating resources to support an effective security program.

Which role normally deals with data recovery and examination after a security breach?

- (●) Digital Forensics Analyst
- ( ) Network Engineers
- ( ) Penetration Tester
- ( ) Security Auditor

Digital Forensic Analysts may be responsible for investigating security incidents and breaches, gathering and analyzing digital evidence, and performing forensic examinations of computer systems, networks, and other digital devices. They may use specialized tools and techniques to recover and examine data from compromised systems, including identifying the cause of the breach and determining the extent of the damage.

Result :

Knowledge Check 4

You will need to achieve a score of 80% or higher to pass the quiz. If you don't pass on your first attempt, you can retake the quiz as needed.

Results

4 of 4 Questions answered correctly

Your time: 00:00:34

You have reached 4 of 4 point(s), (100%)

Click Here to Continue

Restart Quiz