KEAMANAN INFORMASI

FERDIAN AKBAR KURNIAWAN
1310651076
KELAS E

SOAL 1.

DOMAIN 7.

OPERASI KEAMANAN

SENSITIVE INFORMATION/MEDIA SECURITY

keamanan dan kontrol yang terkait dengan orang-orang dalam suatu perusahaan sangatlah penting, sehingga mengalami proses ketat untuk menangani informasi sensitif, termasuk keamanan Media. Bagian ini membahas konsep-konsep yang merupakan komponen penting dari keseluruhan keamanan informasi,

Sensitive information

Informasi sensitif membutuhkan perlindungan, dan informasi yang secara fisik berada pada beberapa bentuk media. Selain penyimpanan utama, penyimpanan cadangan juga harusbdipertimbangkan.

Labeling/marking

Mungkin langkah yang paling penting dalam keamanan media proses menemukan sensitive informasi dan pelabelan atau penandaan sebagai sensitif. Bagaimana data label harus sesuai dengan skema klasifikasi data organisasi.

Handling

Individu orang menangani media sensitif harus dipercaya yang telah diperiksa oleh organisasi. Mereka harus memahami peran mereka dalam informasi organisasi postur keamanan

Storage

Ketika menyimpan informasi sensitif, lebih baik untuk mengenkripsi, pada saat istirahat sangat mengurangi kemungkinan data yang diungkapkan dalam sebuah mode karena masalah keamanan.

Retention

Media dan informasi memiliki masa manfaat yang terbatas. Penyimpanan informasi sensitif

tidak harus bertahan di luar periode kegunaan atau persyaratan hukum (mana yang lebih besar), karena sia-sia memperlihatkan data ancaman pengungkapan ketika data tersebut tidak lagi diperlukan oleh organisasi.

Media sanitization or destruction of data

beberapa data mungkin tidak sensitif dan tidak menjamin kerusakan data menyeluruh, sebuah organisasi akan memiliki data yang harus diverifikasi dihancurkan atau diberikan nonusable dalam kasus media di mana ia ditempatkan dipulihkan oleh pihak ketiga.

ASSET MANAGEMENT

Pendekatan holistik untuk keamanan informasi operasional mengharuskan organisasi untuk fokus pada sistem serta orang, data, dan media.

Configuration management

Dasar Configuration management yang terkait dengan sistem keamanan akan melibatkan tugas-tugas seperti menonaktifkan layanan yang tidak perlu; menghapus program asing.

CONTINUITY OF OPERATIONS

adalah prinsipnya berhubungan dengan porsi ketersediaan kerahasiaan, dan integritas.

Service-Level Agreements

A Service-Level Agreement (SLA) menetapkan semua harapan mengenai perilaku departemen atau organisasi yang bertanggung jawab untuk menyediakan layanan dan kualitas layanan yang diberikan.

Fault tolerance

Agar sistem dan solusi dalam sebuah organisasi untuk dapat terus menyediakan ketersediaan operasional, mereka harus dilaksanakan dengan toleransi kesalahan dalam pikiran.

Backup

Agar data dapat dipulihkan dalam kasus kesalahan, beberapa bentuk cadangan atau redundansi harus disediakan.

Redundant Array of Inexpensive Disks

jika hanya satu tape backup penuh diperlukan untuk pemulihan sistem karena kegagalan hard disk, waktu untuk memulihkan sebagian besar data dapat dengan mudah melebihi pemulihan waktu ditentukan oleh organisasi. Tujuan dari Redundant Array of

Inexpensive Disk (RAID) adalah untuk membantu mengurangi risiko yang terkait dengan kegagalan hard disk. di sana berbagai tingkatan RAID yang terdiri dari pendekatan yang berbeda untuk array disk konfigurasi.

tingkatan RAID yang terdiri dari pendekatan yang berbeda untuk array disk konfigurasi. Meliputi :

RAID 0: Striped set
RAID 1: Mirrored set
RAID 2: Hamming code
RAID 3: Striped set with dedicated parity (byte level)
RAID 4: Striped set with dedicated parity (block level)
RAID 5: Striped set with distributed parity
RAID 6: Striped set with dual distributed parity

INCIDENT RESPONSE MANAGEMENT

Sebuah insiden keamanan adalah kejadian berbahaya pada sistem atau jaringan. semua organisasi akan mengalami insiden keamanan. Manajemen respon insiden sangatlah ketat dan diuji metodologi untuk mengidentifikasi dan merespon insiden ini.

Computer Security Incident Response Team (CSIRT) adalah kelompok yang bertugas pemantauan, mengidentifikasi, dan merespon insiden keamanan.

Malware

Malware, atau kode berbahaya / software, merupakan salah satu jenis yang paling terkenal dari ancaman terhadap sistem informasi.

SOAL 2.

Heartbleed Detector (android)

Better

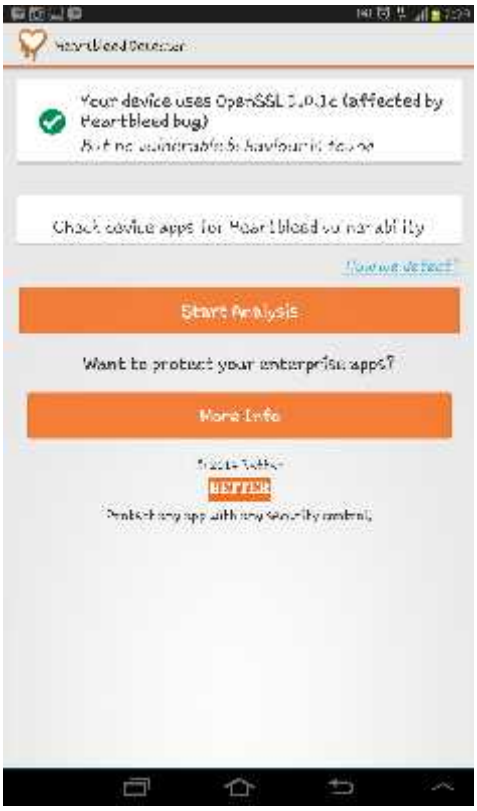
Apa itu HEARTBLEED?

Heartbleed adalah celah keamanan di salah satu ekstensi OpenSSL yang disebut Heartbeat. Celah keamanan ini memungkinkan attacker untuk membaca memory dari server yang diproteksi oleh OpenSSL.

CARA MENGGUNAKAN HEARTBLEED DETECTOR

Install terlebih dahulu aplikasi heartbleed detector,

Setelah terinstall berikut tampilan desktop



Kemudian sentuh start analysis dan tunggu proses sampai selesai mendeteksi

Setelah proses analisis selesai akan tampil gambar berikut