Memantau operasi yang sedang berlangsung dan secara aktif mendeteksi musuh dan melaporkan kasus yang mencurigakan adalah tanggung jawab dari?

Select one:

a. Divisi Deteksi

b. Divisi Menyerang

c. Divisi Monitoring

d. Divisi Bertahan

e. Divisi Pengelola

f. Divisi Respon

Dalam suatu hierarki organisasi IT, CISO merupakan bagian teratas dari IT Security Team. CISO adalah

Select one:

a. Certificate of Intergrated System Object

b. Certificate of Information System Officer

c. Chief Integrated System Operational

d. Certificate Information Security Officer

e. Chief Identity Security Object

f. Chief Information Security Officer

Malicious code yang memiliki karakteristik memungkinkan mengcopy dirinya melalui jaringan komputer adalah:

Select one:

a. Backdoor F. Virus

b. Worm

c. Rabbit

d. salah semua

e. Trapdoor

Yang merupakan bagian dari struktur Security Engineering & Asset Security adalah

Select one:

a. Emergency operations &amp; incedent Management

b. Security Operations Center

c. Personnel &amp; External relationships

d. Govermance, Risk, and Compliance

e. Security Engineering

f. Program Management Office

Yang merupakan tahapan pertama dalam vulnerability assessment adalah

Select one:

a. Balancing the range of enterprise risk

b. Audit &amp; testing documentation examples

c. Chief compliance officer

d. Service infrastructure and application

e. Meeting stakeholder needs

f. Centraized and consolidated

Kriteria yang harus diperhatikan dalam memilih alat Vulnerability Assessment, kecuali ...

Select one:

a. Efisien

b. Alat tersebut berjalan dengan baik

c. Bermanfaat

d. Akurat

e. Miliki kapabilitas pada saat tes berlangsung

Kualitas dari keaslian adalah salah satu faktor yang diperhatikan. Baik dari segi komunikasi, dokumen yang tersedia maupun data yang ada adalah pengertian dari salah satu elemen keamanan informasi yaitu

Select one:

a. Keutuhan

b. Keaslian

c. Keamanan

d. Ketersediaan

e. Non Repudiasi

f. Kerahasiaan

Mengapa diperlu analisa kelemahan:

Select one:

a. Data dan iformasi terus meningkat

b. Mengetahui Data dan informasi

c. Data Breach Staristics yang normal

d. Kebocoran data dan informasi semakin meningkat

e. Untuk meningkatkan informasi

f. Untuk mendeteksi kelemahan

Memungkinkan untuk mengakses secara jarak jauh/remote jaringan tertentu dan menentukan jaringan tersebut rusak atau disalahgunakan. Adalah penjelasan dari ...

Select one:

a. GFI LANGuard

b. Retina Network Security Scanner

c. MBSA

d. Nessus

e. SAINT Vulnerability Scanner

Bagian dari penilaian dari satu sistem apakah memiliki kelemahan ataupun tidak adalah definisi dari

Select one:

a. Deteksi

b. Keutuhan

c. Keaslian

d. Analisa

e. Kelemahan

f. Ketersediaan

Berikut ini adalah salah satu tipe assessment adalah

Select one:

a. Host Based Assessment

b. Availability Assessment

c. Risk Assessment

d. Integrity Assessment

e. Compliance Assessment

f. Confidential Assessment

Availability adalah

Select one:

a. Informasi hanya dapat diakses oleh yang berhak

b. Tidak bisa disangkal bahwa informasi memang berasal dari orang yang bersangkutan

c. Isi data/ informasi tidak berubah

d. Data/ informasi berasal dari orang yang benar

e. Data/ informasi tersedia saat dibutuhkan

f. Tidak ada

Bagian dari penilaian terhadap area yang dilakukan penilaian adalah definisi dari

Select one:

a. Kelemahan

b. Analisa

c. Keutuhan

d. Keaslian

e. Deteksi

f. Ketersediaan

Salah satu produk untuk keamanan dalam pengiriman email dengan membangun key ring adalah:

Select one:

a. Routing problem

b. Smtp

c. Pretty good provacy

d. Salah semua

e. Disruption of Services

f. Pop3

Berikut ini yang merupakan tahap pertama pada alur penanganan insiden adalah

Select one:

a. Training and Awareness

b. Handling Insident

c. Goals of Incedent Response

d. Need for Incedent Response

e. Incident Response Best Practices

f. Insident Response Plan

Ketersediaan informasi yang ada menjadi faktor utama apakah informasi tersebut dapat di simpan, proses dan di sebarkan oleh pihak yang hanya diijinkan adalah pengertian dari salah satu elemen keamanan informasi yaitu

Select one:

a. Ketersediaan

b. Non Repudiasi

c. Keutuhan

d. Keaslian

e. Kerahasiaan

f. Keamanan

Berikut ini tugas dari divisi monitoring adalah

Select one:

a. Recover

b. Sustain

c. Hunt

d. Respond

e. Govern

f. Manage Risk

ada dua pendekatan Vulnerability Assessment , yaitu

Select one:

a. Product-Based Assessment dan Service-Based Vulnerability

b. Service-Based dan Product-Based Vulnerability

c. Service-Based dan Product-Based

d. Service-Based Assessment dan Product-Based Vulnerability

e. Product-Based dan Service-Based Assessment

f. Product-Based dan Service-Based Vulnerability

Yang merupakan tanggung jawab dari divisi pengelola adalah

Select one:

a. cepat meminimalkan dampak dan memastikan bahwa organisasi cepat dikerahkan untuk mengembalikan aset kedalam kondisi normal

b. Memastikan bahwa pimpinan organisasi, staf, kebijakan, proses, praktek, dan teknologi memberikan pengawasan yang berkelanjutan, manajemen, pengukuran, kenerja dan mengoreksi semua kegiatan di cybersecurity

c. monitor, hunt &amp; detect

d. problem solve

e. respon &amp; recover

f. protect, defend, shield &amp; prevent

Layer enam pada pertahanan informasi adalah

Select one:

a. Data

b. Aplikasi

c. Perimeter

d. Host

e. Fisikal

f. Jaringan internal

Salah satu keuntungan yang didapatkan dari deteksi sebuah kelemahan sejak awal adalah

Select one:

a. Menambah kesadaran untuk mengurangi tingkat keamanaan data

b. Mengurangi kerusakan data

c. mengakibatkan adanya insiden

d. Memperlambat proses incident handling

e. Memberikan pengetahuan dari keabsahan bahwa system tersebut digunakan atau tidak

f. Memastikan system teregister dengan baik

Berikut ini aspek yang diperlukan dari vulnerability assessment adalah

Select one:

a. Mengklasifikasi kunci aset dan manajemen resiko

b. Evaluasi ketahap Pentest

c. Menjadwalkan asset

d. Mengidefikasi kelemahan dari sistem

e. Mengidentifikasi kerentanan

f. Mengidentifikasi Area

Bentuk-bentuk klasifikasi dari kelemahan adalah berikut ini, kecuali?

Select one:

a. Kelemahan sistem operasi

b. Enkripsi

c. Buffer overflows

d. Password standar

e. Servis yang terbuka

f. Kelemahan design

Menilai level dari dampak adalah termasuk tahap

Select one:

a. Impact Analysis

b. Incident Handling

c. Risk Assessment

d. Monitoring

e. Verification

f. Remediation

Aspek kejahatan komputer yang termasuk akses orang ke gedung, peralatan & media yang digunakan adalah merupakan:

Select one:

a. Keamanan peralatan

b. Keamanan yang berhubungan dengan orang

c. Keamanan dari data &amp; media

d. Keamanan Informasi

e. Keamanan bersifat fisik operasi

f. Keamanan dalam sistem

Yang bukan termasuk contoh kelemahan adalah

Select one:

a. Kelemahan sistem operasi

b. DOS

c. Buffer Overflows

d. Instalasi standar

e. Kelemahan desain

f. Kelemahan aplikasi

Deteksi dan analisa kelemahan pada suatu organisasi oleh pihak internal dilakukan oleh

Select one:

a. IT security team

b. Chief Information Security

c. Response team

d. IT engineer

e. Network engineer team

f. Monitoring team

Berapa tahapan standar untuk melakukan Vulnerability Assessment yang harus diperhatikan

Select one:

a. 7

b. 9

c. 8

d. 5

e. 3

f. 6

Inurl:.php site:kemhan.go.id maksud pencarian tersebut adalah

Select one:

a. Membuat extension .php pada website kemhan

b. Mencari website kemhan.go.id

c. Mencari website kemhan yang bukan berextension .php

d. Mengcopy extension .php pada website kemhan

e. Mencari extension .php pada website kemhan

f. Menyalin extension .php pada website kemhan

Tahapan berikut yang termasuk dalam tahapan vulnerability assessment adalah

Select one:

a. Mengklasifikasi kunci aset dan manajemen resiko

b. Mengidentifikasi Area

c. Evaluasi ketahap Pentest

d. Mengidentifikasi kerentanan

e. Mengidefikasi kelemahan dari sistem

Berikut ini yang bukan termasuk ke dalam layer pertahanan informasi adalah

Select one:

a. Data

b. Jaringan Internal

c. Perimeter

d. Host

e. Jaringan Eksternal

f. Aplikasi

Berikut ini yang tidak termasuk tahapan vulnerability assessment adalah

Select one:

a. Create a vulnerability scan report

b. Identify and prioritize vulnerabillities

c. Check for misconfigurations

d. Disable vulnerability scans

e. Examine and evaluate physical security

f. Apply business and technology context to scanner results

Serangan Hacker yang mengakibatkan miliaran data para pemakai jasa bocor:

Select one:

a. JPMorganChase

b. Trojan

c. Malware

d. JPMorganchasa

e. DDos

f. Attack

Jenis tools yang digunakan untuk menemukan dan mengidentifikasi kerentanan sistem yang tidak diketahui sebelumnya adalah?

Select one:

a. Depth assessment tools

b. Host-based vulnerability tools

c. Scope assessment tools

d. Web based assessment tools

e. Application layer vulnerability assessment tools

f. Patial assessment tools

Berikut fase yang tepat saat setelah adanya penilaian

Select one:

a. remediation - risk assessment - verification - monitoring

b. risk assessment - verification - remediation - monitoring

c. monitoring - verification - remediation - risk assessment

d. monitoring - remediation - verification - risk assessment

e. verification - monitoring - risk assessment - remediation

f. risk assessment - remediation - verification - monitoring

Pada alur penanganan insiden, tahapan setelah Handling Incident adalah…

Select one:

a. Incident Response and Handling Steps

b. Goal of Incident Response

c. Incident Management

d. Need for Incident Response

e. Incident Response Plan

f. Training and Awareness

Yang merupakan alur kerja dari ScanningVulnerability adalah

Select one:

a. Perform Service – Locate Node – Test Service

b. Locate Node – test Service – perform Service

c. Locate Node – Perform Service – Test Service

d. Test Service – Perform Service – Locate Node

e. Test Service – Locate Node – Perform Service

f. Perform Service – Test Service – Locate Node

Berikut ini yang tidak termasuk tools untuk vulnerability assessment adalah

Select one:

a. QualysGuard

b. SAINT Vulnerability Scanner

c. Ettercap

d. Nessus

e. GFI LANGuard

f. Retina Network Security Scanner

Dibawa ini contoh dari tahapan vulnerability assessment adalah

Select one:

a. Risk Assessment, Creating Baseline

b. Risk Assessment, Risk Management

c. Risk Control, Monitor

d. Risk Management, Creating Baseline

e. Compliance, Remediation

f. Risk Authentication, Risk Control

Jenis-jenis Vunerability Assessment adalah :

Select one:

a. Network assessment

b. Integrity

c. Non Repudiation

d. Availability

e. Transmission

f. Confidentiality

Dibawah ini merupakan 5 fase dalam melakukkan vulnerability assessment adalah

Select one:

a. Report, System, Planning, Analysis, Final Report

b. Planning, Visit, Analysis, Draft Report, Final Report

c. Analysis, Client, System, Draft Report, Final Report

d. Planning, Visit, Risk, System, Final

e. Risk, System, Final Report, Draft Report, Client

f. Clients, Draft, Report, System, Plan

Di bawah ini yang tidak termasuk jenis-jenis alat vulnerability assessment adalah ?

Select one:

a. Scope assessment tools

b. Depth assessment tools

c. Application-layer vulnerability assessment tools

d. Host-based vulnerability assessment tools

e. Client Assessment tools

Empat elemen keamanan informasi kecuali

Select one:

a. kerahasiaan

b. non-repudasi

c. kerentanan

d. keutuhan

e. ketersediaan

f. keaslian

Keuntungan dilakukannnya vulnerability assessment adalah sebagai berikut

Select one:

a. untuk mengganti system yang tidak baik

b. melemahkan system yang ada

c. hanya mengetahui dan menguji kelemahan system yang ada tanpa tindak lanjut

d. mendapatkan celah untuk melakukan serangan ke system yang ada

e. memperoleh gambaran untuk membangun system yang lebih baik

f. Memberikan kesadaran bahwa sistem yang digunakan memiliki kelemahan atau tidak

Lokasi kelemahan terdeteksi oleh scanner yaitu pada code

Select one:

a. SSH

b. HTTPS

c. FTP

d. TCP

e. HTTP

f. HTML

Layer lima pada pertahanan informasi adalah

Select one:

a. Aplikasi

b. Host

c. Jaringan Internal

d. Fisikal

e. Data

f. Perimeter

Berikut ini yang bukan merupakan tujuan dari vulnerability assessment adalah?

Select one:

a. Mengidentifikasi kerentanan

b. Evaluasi ketahap pentest

c. Mengklasifikasi kunci aset dan manajemen resiko

d. Mengidentifikasi area

e. Mengidentifikasi kelemahan dari sistem

f. Persiapan melakukan serangan balik ke penyerang sistem

Yang termasuk klasifikasi dalam kelemahan, kecuali

Select one:

a. Kesalahan dalam konfigurasi

b. Buffer Overflows

c. Instalasi Standar

d. Server tidak pernah di patch/update

e. Password standar

f. Network Design

Dapat mendeteksi dan melakukan scan terhadap network dan port serta mendeteksi kelemahan keamanan. Adalah penjelasan dari ...

Select one:

a. SAINT Vulnerability Scanner

b. MBSA

c. GFI LANGuard

d. Nessus

e. Retina Network Security Scanner

Dibawah ini beberapa hal yang harus diketahui dari ketersediaan informasi, kecuali

Select one:

a. Risk Management

b. Perimeter

c. Aplikasi

d. Data

e. Fisikal

f. Host