Mengidentifikasi kelemahan pada network device, operating system, desktop applications, web applications, database. Alat ini menemukan dan memperbaiki kemungkinan kelemahan pada jaringan keamanan sebelum di eksploit. Adalah penjelasan dari ...

Select one:

a. MBSA



b. Retina Network Security Scanner



c. GFI LANGuard



d. Nessus



e. SAINT Vulnerability Scanner



Layer lima pada pertahanan informasi adalah

Select one:

a. Fisikal



b. Jaringan Internal



c. Host



d. Perimeter



e. Aplikasi



f. Data



Berikut fase yang tepat saat setelah adanya penilaian

Select one:

a. monitoring - verification - remediation - risk assessment



b. risk assessment - verification - remediation - monitoring



c. risk assessment - remediation - verification - monitoring



d. remediation - risk assessment - verification - monitoring



e. monitoring - remediation - verification - risk assessment



f. verification - monitoring - risk assessment – remediation



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

Select one:

a. Mencari extension .php pada website kemhan



b. Mencari website kemhan.go.id



c. Membuat extension .php pada website kemhan



d. Menyalin extension .php pada website kemhan



e. Mencari website kemhan yang bukan berextension .php



f. Mengcopy extension .php pada website kemhan



Empat elemen keamanan informasi kecuali

Select one:

a. kerahasiaan



b. kerentanan



c. ketersdiaan



d. keaslian



e. non-repudasi



f. keutuhan



Berikut ini yang tidak termasuk tahapan vulnerability assessment adalah

Select one:

a. Identify and prioritize vulnerabillities



b. Create a vulnerability scan report



c. Check for misconfigurations



d. Disable vulnerability scans



e. Examine and evaluate physical security



f. Apply business and technology context to scanner results



Orang yang paling bertanggung jawab dalam unit organisasi pengelola deteksi dan analisa kelemahan adalah?

Select one:

a. CIO (Chief Information Officer/HRD(?))



b. CSO (Chief Security Officer)



c. CEO



d. CISO (Chief Information security Officer)



e. CMO (Chief Marketing Officer)



f. CTO (Chief Technology Officer)



Tanggung jawab dari defense adalah

Select one:

a. problem solve



b. protect, defend, shield &amp; prevent



c. manage risk



d. monitor, hunt &amp; detect



e. manage &amp; educate



f. respon &amp; recover



Berikut ini tujuan keamanan informasi yang benar adalah

Select one:

a. Kerahasiaan, kesinambungan, estetika



b. Keabsahan, ketersediaan, estetika



c. Kerahasiaan, ketersediaan, estetika



d. Keabsahan, ketersediaan,integritas



e. Kerahasiaan, ketersediaan, integritas



f. Kerahasiaan, kesinambungan, integritas



Proses pengujian kemampuan dari suatu system atau aplikasi disebut

Select one:

a. Scanning Assessment



b. Managing Risk Assessment



c. Vulnerability Assessment



d. Sniffing Assessment



e. Detecting Assessment



f. Spoofing Assessment



Empat elemen keamanan informasi kecuali

Select one:

a. ketersdiaan



b. kerahasiaan



c. keaslian



d. non-repudasi



e. kerentanan



f. keutuhan



Terdapat beberapa komponen pemebentuk deteksi di bawah ini, kecuali?

Select one:

a. Deteksi Pasif



b. Deteksi Aktif



c. Otomatis dan Manual



d. Pencarian informasi



e. Pengumpulan informasi



f. Penarikan informasi



Yang tidak termasuk kedalam bagian dari jenis Vulnerability Assesment

Select one:

a. Passive Assessment



b. Active Assessment



c. Client – Server Assessment



d. Extenal Assessment



e. Internal Assessment



f. Network Assessment



Di bawah ini yang tidak termasuk Jenis-jenis analisa kelemahan teknologi informasi adalah ?

Select one:

a. Analisa kelemahan pada Jaringan



b. Analisa kelemahan pada data



c. Analisa kelemahan pada aplikasi



d. Analisa kelemahan pada servis



e. Analisa kelemahan pada infrastruktur



Memastikan bahwa organisasi staf, kebijakan, proses, praktek, dan teknologi memantau operasi yang sedang berlangsung dan secara aktif mendeteksi musuh dan melaporkan kasus yang mencurigakan dan tidak sah secepat mungkin adalah tanggung jawab dari divisi

Select one:

a. Pengelola



b. Respon



c. Bertahan



d. Govern



e. Monitoring



f. CISO



Berikut ini aspek yang diperlukan dari vulnerability assessment adalah

Select one:

a. Mengidentifikasi Area



b. Evaluasi ketahap Pentest



c. Menjadwalkan asset



d. Mengidentifikasi kerentanan



e. Mengklasifikasi kunci aset dan manajemen resiko



f. Mengidefikasi kelemahan dari sistem



Yang tidak termasuk kedalam kelemahan dalam sistem adalah

Select one:

a. Password standar



b. Tidak adanya antivirus



c. Kelemahan Service



d. Instalasi Standar



e. Kelemahan Design sistem



f. Server tidak pernah di update



Langkah awal vulnerability assessment adalah

Select one:

a. Mengecek misconfiguration



b. Membuat laporan vulnerability



c. Identifikasi prioritas vulneraility



d. Menjalankan OSINT



e. Mengevaluasi physical security



f. Menjalankan vulnerability scan



Berikut ini tugas dari divisi pengelola adalah

Select one:

a. Sustain (div.Respon



b. Recover(div.Respon



c. Respond



d. Hunt



e. Educate



f. Monitor



Teknik penncarian informasi secara passif adalah

Select one:

a. Teknik penca



b. Audit



c. Complience



d. Application



e. Loging



f. Integrity



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

Select one:

a. Scope assessment tools



b. Host-based vulnerability assessment tools



c. Client Assessment tools



d. Depth assessment tools



e. Application-layer vulnerability assessment tools



Yang merupakan layer pertahanan informasi adalah

Select one:

a. Datalink layer



b. Transport layer



c. Network layer



d. Presentation layer



e. Physical layer



f. Sesion layer



ada dua pendekatan Vulnerability Assessment , yaitu

Select one:

a. Service-Based dan Product-Based Vulnerability



b. Service-Based Assessment dan Product-Based Vulnerability



c. Service-Based dan Product-Based



d. Product-Based dan Service-Based Assessment



e. Product-Based Assessment dan Service-Based Vulnerability



f. Product-Based dan Service-Based Vulnerability



GFI LANGuard dapat mendeteksi dan melakukan scan terhadap :

Select one:

a. kelemahan



b. network dan port



c. alamat IP



d. topologi



e. aplikasi



f. design network



Dibawa ini contoh dari tahapan vulnerability assessment adalah

Select one:

a. Risk Authentication, Risk Control



b. Risk Assessment, Risk Management



c. Compliance, Remediation



d. Risk Assessment, Creating Baseline



e. Risk Management, Creating Baseline



f. Risk Control, Monitor



Fungsi keseluruhan dari CISO adalah

Select one:

a. bertahan dari segala serangan



b. membuat supaya semua control dapat berjalan



c. menjaga keseluruhan keamanan informasi pada suatu organisasi



d. mengaja ketersediaan data yang ada



e. mengerjakan semua pengamanan informsi



f. hanya menjaga kerahasiaan informasi



Yang bukan alasan menggunakan vulnerability assessment adalah :

Select one:

a. Suatu peristiwa yang akan terjadi, tetapi tidak mungkin terjadi



b. Suatu peristiwa yang bisa terjadi, dan sudah terjadi terjadi



c. Mengidentifikasi kerentanan



d. Mengidentifikasi Area



e. Suatu peristiwa yang tidak akan terjadi, tidak mungkin terjadi



f. Mengevaluasi hasil pentest



Yang merupakan layer pertama pada pertahanan informasi adalah

Select one:

a. data



b. host



c. kebijakan,prosedur,dan kesadaran



d. aplikasi



e. jaringan internal



f. perimeter



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

:

a. Divisi Respon



b. Divisi Deteksi



c. Divisi Bertahan



d. Divisi Monitoring



e. Divisi Menyerang



f. Divisi Pengelola



Yang merupakan tanggung jawab dari divisi pengelola adalah

Select one:

a. respon &amp; recover



b. protect, defend, shield &amp; prevent



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



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



e. monitor, hunt &amp; detect



f. problem solve



Alat yang didesain untuk IT professional yang dapat membantu bisnis kecil atau besar untuk menentukan keamanan sesuai dengan recomendasi keamanan microsoft. Adalah penjelasan dari ...

Select one:

a. SAINT Vulnerability Scanner



b. MBSA



c. GFI LANGuard



d. Nessus



e. Retina Network Security Scanner



Proses setelah Risk Assessment pada proses Vulnerability Assessment adalah…

Select one:

a. Creating Baseline



b. Monitor



c. Attack



d. Remediation



e. Vulnerability Assessment



f. Verification



Berikut ini fungsi dari CISO kecuali:

Select one:

a. Monitor



b. Gonvern



c. Sustain



d. Attack



e. Detect



f. Protect



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

Select one:

a. Kelemahan



b. Keaslian



c. Keutuhan



d. Deteksi



e. Analisa



f. Ketersediaan



Dibawah ini yang bukan fase sebelum penilaian..

Select one:

a. Define the scope of the assessments



b. Map the network infrastructure



c. Identify the controls already in place



d. Create an inventory of all assets, and rank the critical assets



e. Run vulnerability scans using tools



f. Identify and understand business procesess



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 Information Security Officer



c. Chief Identity Security Object



d. Chief Integrated System Operational



e. Certificate of Information System Officer



f. Chief Information Security Officer



Mengapa diperlu analisa kelemahan:

Select one:

a. Untuk meningkatkan informasi



b. Data dan iformasi terus meningkat



c. Data Breach Staristics yang normal



d. Untuk mendeteksi kelemahan



e. Kebocoran data dan informasi semakin meningkat



f. Mengetahui Data dan informasi



Apa yang di maksud dengan retina network security ?

Select one:

a. Salah satu alat bantu untuk pencarian kelemahan



b. Salah satu alat bantu untuk ,mendeteksi kerentanan



c. Salah satu alat bantu untuk melakukan penetration testing



d. Salah satu alat bantu untuk uji coba kerentanan



e. Salah satu alat bantu untuk Menciptakan serangan



Yang termasuk klasifikasi dalam kelemahan, kecuali

Select one:

a. Instalasi Standar



b. Buffer Overflows



c. Network Design



d. Password standar



e. Kesalahan dalam konfigurasi



f. Server tidak pernah di patch/update



Yang bukan termasuk contoh kelemahan adalah

Select one:

a. Instalasi standar



b. Kelemahan sistem operasi



c. Kelemahan desain



d. DOS



e. Kelemahan aplikasi



f. Buffer Overflows



Berikut ini yang bukan termasuk ke dalam layer pertahanan informasi adalah

Select one:

a. Perimeter



b. Jaringan Internal



c. Jaringan Eksternal



d. Aplikasi



e. Host



f. Data



Layer tiga pada pertahanan informasi adalah

Select one:

a. Host



b. Jaringan Internal



c. Perimeter



d. Fisikal



e. Aplikasi



f. Data



Yang merupakan bagian dari struktur Security Engieering & Asset Security adalah

Select one:

a. Program Management Office



b. Govermance, Risk, and Compliance



c. Security Operations Center



d. Emergency operations &amp; incedent Management



e. Personnel &amp; External relationships



f. Security Engineering



Harus memahami dan mengidentifikasi proses bisnis pada sistem yang akan di uji, serta mengetahui peta infrastruktur jaringan dan lainnya merupakan proses vulnerability

Select one:

a. risk assessment



b. minitoring



c. fase sebelum penilaian



d. fase setelah penilaian



e. remediation



f. verivication



Layer enam pada pertahanan informasi adalah

Select one:

a. Host



b. Jaringan internal



c. Perimeter



d. Fisikal



e. Data



f. Aplikasi



Berikut ini yang merupakan tahap kedua pada alur penanganan insiden adalah

Select one:

a. Need for Incedent Response



b. Handling Insident



c. Goals of Incedent Response



d. Training and Awareness



e. Insident Response Plan



f. Incident Response Best Practice



Yang tidak termasuk dalam proses penilaian kelemahan adalah

Select one:

a. Verification



b. Monitor



c. Risk Assessment



d. Remediation



e. Analisys



Keutuhan dari informasi untuk mencegah informasi dapat diganti dan diakses oleh pihak yang tidak berwenang adalah pengertian dari salah satu elemen keamanan informasi yaitu

Select one:

a. Non Repudiasi



b. Kerahasiaan



c. Ketersediaan



d. Keutuhan



e. Keamanan



f. Keaslian



Tidak adanya perubahan pada informasi yang dikirimkan disebut juga dengan

Select one:

a. Creation



b. Authentication



c. Integrity



d. Availablelity



e. Confidentiality



f. Migitation

