1-کدام یک از ویژگی های IDS صحیح است؟

الف) فقط برای شناسایی تهدیدات استفاده میشود و اقدامی برای جلو گیری انجام نمی دهد ☑ .

ب) اقداماتی برای جلوگیری از حملات انجام می دهد.

ج) برای جلوگیری از نفوذ به شبکه استفاده می شود.

د) از داده ها رمزنگاری می کند.

پاسخ گزینه الف

2-کدام یک از ویژگی های IPS صحیح است؟

الف) فقط تهدیدات را شناسایی می کند.

ب) اقداماتی برای جلوگیری از حملات انجام می دهد ☑ .

ج) برای حفاظت از اطلاعات درون سازمانی استفاده می شود.

د) به طور خودکار داده ها را رمزنگاری می کند.

پاسخ گزینه ب

3-ترجمه آدرس شبکه (NAT) چه مزیتی در امنیت شبکه دارد؟

الف) پنهان سازی آدرس IP داخلی دستگاه ها ☑

ب) رمزنگاری داده ها در شبکه

ج) نظارت بر ترافیک شبکه

د) شناسایی تهدیدات در شبکه

پاسخ گزینه الف

سوالات امنیت داده (آزمون استخدامی)

4-کدام یک از ویژگی های امنیتی IPSec است؟

الف) رمزنگاری بسته های داده ☑

ب) شناسایی تهدیدات در شبکه

ج) نظارت بر فعالیت های سیستم

د) پنهان سازی آدرسIP

پاسخ گزینه الف

5-کدام یک از پروتکل های امنیتی در شبکه های بی سیم قدیمی ترین و با امنیت پایین تر است؟

WPA3

WPA

WEP ☑

WPA2

پاسخ گزینه: ج

6-کدام یک از اقدامات امنیتی برای شبکه های بی سیم میتواند به کاهش احتمال نفوذ کمک کند؟

الف)استفاده ازIPS

ب) استفاده ازNAT

ج) نصبIDS

د) استفاده از فیلتر MAC ☑

پاسخ گزینه: د

دانلود سوالات استخدامی امنیت داده

7-اصل تفکیک وظایف در امنیت پایگاه داده به چه هدفی پیاده سازی می شود؟

الف) کاهش حجم داده ها

ب) جلوگیری از کنترل کامل یک کاربر بر داده ها☑

ج) رمزنگاری داده های حساس

د) جلوگیری از دسترسی غیر مجاز

پاسخ گزینه ب

8-کدام اصل امنیتی تضمین میکند که هر کاربر تنها به میزان دسترسی مورد نیاز خود دسترسی داشته باشد؟

الف) تفکیک وظایف

ب) نرمال سازی ایمن

ج) حداقل امتیاز☑

د) طبقه بندی داده ها

پاسخ گزینه : ج

9-تفکیک محیط های توسعه تست و تولید چه کمکی به امنیت پایگاه داده می کند؟

الف) کاهش تکرار داده ها

ب) جلوگیری از حملات داخلی

ج) بهبود عملکرد پایگاه داده

د) افزایش امنیت داده های واقعی ☑

پاسخ گزینه د

دانلود رایگان سوالات استخدامی امنیت داده

10-کدام یک از رویکردهای امنیتی برای حفاظت از داده ها در حین انتقال مناسب است؟

الف) نرمال سازی ایمن

ب) رمزنگاری ☑

ج) مدیریت کلید

RBAC

پاسخ گزینه ب

11-استفاده از دستورات SQL پارامتریک چه کمکی به امنیت پایگاه داده می کند؟

الف) جلوگیری از تزریق SQL ☑

ب) کاهش حجم داده ها

ج) کاهش خطای انسانی

د) بهبود کارایی پایگاه داده

پاسخ گزینه الف

12-ابزارهای SIEM چه نقشی در امنیت پایگاه داده ایفا می کنند؟

الف) تحلیل لاگها برای شناسایی رفتارهای مشکوک ☑

ب) کنترل دسترسی به جداول

ج) طبقه بندی داده ها

د) مدیریت کلیدهای رمزنگاری

پاسخ گزینه الف

13-کدام یک از ویژگیهای ABAC در کنترل دسترسی پایگاه داده صحیح است؟

الف) دسترسی ها بر اساس نقش ها تعیین می شود.

ب) دسترسی ها بر اساس ویژگیهای کاربران یا شرایط محیطی تنظیم می شوند ☑ .

ج) دسترسی ها تنها به ستونهای مشخصی از جدول محدود می شوند.

د) دسترسی ها بر اساس مدل نرمال سازی داده ها تنظیم می شوند.

پاسخ گزینه ب

14-پنهان سازی داده ها (Data Masking) چه کاربردی دارد؟

الف) جایگزینی داده های حساس با مقادیر ساختگی ☑

ب) رمزنگاری داده های حساس

ج) افزایش کارایی پایگاه داده

د) کنترل دسترسی به جداول

پاسخ گزینه الف

15-مدیریت کلیدهای رمزنگاری چگونه به امنیت پایگاه داده کمک می کند؟

الف) کاهش زمان پردازش کونری ها

ب) جلوگیری از افشای داده ها ☑

ج) افزایش کارایی پایگاه داده

د) بهبود مدیریت کاربران

پاسخ گزینه ب

16-حملات SQL Injection چگونه انجام می شود؟

الف) از طریق تزریق داده های غیر مجاز به کونری های SQL ☑

ب) از طریق دسترسی غیر مجاز به کلیدهای رمزنگاری

ج) از طریق پنهان سازی آدرسIP

د) از طریق تغییر لاگ های پایگاه داده

پاسخ گزینه الف

سوالات استخدامی امنیت داده با جواب

17-طبقه بندی داده ها در پایگاه داده چه نقشی دارد؟

الف) بهبود سرعت پردازش داده ها

ب) افزایش دقت کونری ها

ج) کاهش حجم پایگاه داده

د) تعیین سطوح امنیتی مختلف برای داده ها ☑

پاسخ گزینه د

18-استفاده از الگوریتم AES در رمزنگاری داده ها چه مزیتی دارد؟

الف) سرعت بالا در رمزنگاری

ب) امنیت بالا برای داده های حساس ☑

ج) استفاده کمتر از منابع سخت افزاری

د) کاهش نیاز به پنهان سازی داده ها

پاسخ گزینه ب

19-فایروال پایگاه داده چگونه به امنیت کمک می کند؟

الف) ایجاد لایه ای بین کاربران و داده ها برای شناسایی و جلوگیری از کونری های مشکوک ☑

ب) طبقه بندی داده ها بر اساس حساسیت

ج) مدیریت کاربران و نقش ها

د) نظارت بر عملکرد پایگاه داده

پاسخ گزینه الف

20-اجر از هویت دو عاملی (FA) چه نقشی در امنیت پایگاه داده دارد؟

الف) افزایش سرعت دسترسی به داده ها

ب) بهبود کارایی نقش ها و مجوزها

ج) کاهش احتمال دسترسی غیر مجاز به پایگاه داده ☑

د) بهبود الگوریتم های رمزنگاری

پاسخ گزینه ج

21-کدام یک از مراحل در چرخه حیات توسعه نرم افزار امن (Secure SDLC) به شدت بر شناسایی آسیب پذیری ها قبل از انتشار نرم افزار تمرکز دارد؟

الف) توسعه امن

ب) تست امنیتی ☑

ج) نگهداری و نظارت امنیتی

د) طراحی امن

پاسخ گزینه ب

تست های استخدامی امنیت داده

22-کدام نوع بد افزار برای جمع آوری اطلاعات کاربر به طور مخفیانه از سیستم استفاده می کند؟

الف) ویروس

ب) تروجان

ج) جاسوس افزار ☑

د) باج افزار

پاسخ گزینه ج

23-کدام یک از روش های مقابله با حملات DDoS برای توزیع بار به سرورهای مختلف و کاهش فشار بر سرور هدف استفاده می شود؟

الف) استفاده از CDN ☑

ب) اعمال سیاستهای امنیتی مانند تأیید هویت دو مرحله ای

ج) استفاده از ابزارهای آنتی ویروس

د) استفاده از فایروال های شخصی

پاسخ گزینه: الف

24-در تحلیل حملات سایبری کدام مرحله به بررسی و تحلیل دقیق روش ها، تکنیک ها و ابزارهای استفاده شده توسط مهاجم اشاره دارد؟

الف) شناسایی رخداد

ب) تحلیل رفتار مهاجم☑

ج) حذف تهدید

د) جمع آوری شواهد

پاسخ گزینه ب

25-کدام اقدام در هنگام رخدادهای امنیتی به جلوگیری از گسترش آسیب و محدود کردن دسترسی مهاجم به دیگر بخش های شبکه اشاره دارد؟

الف) شناسایی رخداد

ب) بازیابی سیستم

ج) حذف تهدید

د) مهار حمله☑

پاسخ گزینه: د

26-در فرآیند مدیریت رخدادهای امنیتی کدام مرحله به ارزیابی و تعیین شدت و گستره حمله اشاره دارد؟

الف) ارزیابی تأثیر ☑

ب) شناسایی رخداد

ج) حذف تهدید

د) بازیابی

پاسخ گزینه الف

27-کدام یک از اصول رمزنگاری برای تضمین این که داده ها تنها برای افراد مجاز قابل دسترسی باشند، استفاده می شود؟

الف) یکپارچگی

ب) احراز هویت

ج) محرمانگی ☑

د) تأسیس هویت

پاسخ گزینه : ج

28-کدام نوع رمزنگاری از دو کلید مجزا یکی برای رمزنگاری داده ها و دیگری برای رمز گشایی، استفاده می کند؟

الف) رمزنگاری متقارن

ب) رمزنگاری نامتقارن ☑

ج) رمزنگاری ترکیبی

د)رمزنگاری بلوک

پاسخ گزینه ب