

قسمتی از سوالات : استخدامی امنیت شبکه (برای آزمون استخدامی)

- کدام یک از مراحل مدیریت ریسک شامل تحلیل دقیق اطلاعات شناسایی شده و ارزیابی احتمال وقوع تهدیدات است؟

الف) شناسایی ریسک‌ها

☒ ب) ارزیابی ریسک‌ها

ج) اجرای اقدامات کاهش ریسک

د) پایش و بازبینی

- کدام یک از پروتکل‌های زیر برای رمزنگاری داده‌ها در هنگام انتقال در شبکه استفاده می‌شود؟

☒ الف) SSL/TLS

ب) DES

ج) AES

د) RSA

- کدام یک از موارد زیر از وظایف اصلی یک مرکز عملیات امنیتی (SOC) است؟

الف) مدیریت رمزنگاری داده‌ها

☒ ب) تحلیل تهدیدات و پاسخ‌دهی به رخدادها

ج) ایجاد سیاست‌های امنیتی

د) توسعه ابزارهای نظارت امنیتی

- کدام یک از مراحل تست نفوذ به شبیه‌سازی حملات واقعی و تلاش برای دسترسی غیرمجاز به

سیستم پرداخته می‌شود؟

الف) شناسایی آسیب‌پذیری‌ها

ب) برنامه‌ریزی و شناسایی

☒ ج) ارزیابی تأثیر

د) بهره‌برداری (Exploitation)

- کدام یک از ابزارهای زیر برای تجزیه و تحلیل لاگ‌ها و شناسایی تهدیدات در شبکه‌ها و

سیستم‌ها استفاده می‌شود؟

☒ الف) QRadar

ب) BitLocker

ج) Open VPN

د) Apache

– کدام اقدام در هنگام رخدادهای امنیتی به جلوگیری از گسترش آسیب و محدود کردن دسترسی مهاجم به دیگر بخش‌های شبکه اشاره دارد؟

الف) شناسایی رخداد

ب) بازیابی سیستم

ج) حذف تهدید

☒ د) مهار حمله

– کدام یک از مراحل تست نفوذ شامل شناسایی نقاط ضعف سیستم قبل از سوءاستفاده مهاجمان واقعی می‌شود؟

الف) برنامه‌ریزی و شناسایی

ب) بهره‌برداری (Exploitation)

☒ ج) شناسایی آسیب‌پذیری‌ها

د) تهیه گزارش

– کدام یک از ابزارها برای نظارت و تحلیل رفتارهای مشکوک در پایگاه داده استفاده می‌شود؟

الف) RBAC

ب) نرمال‌سازی ایمن

ج) HSM

☒ د) فایروال پایگاه داده

– کدام نوع بدافزار برای جمع‌آوری اطلاعات کاربر به طور مخفیانه از سیستم استفاده می‌کند؟

الف) ویروس

ب) تروجان

☒ ج) جاسوس افزار

د) باج افزار