بررسی ساختار دامنه ششم CISSP

ذهنیت سازی ارزیابی و آزمون امنیتی

دامنه ششم

Security Assessment and Testing

6

دامنه 6 از آزمون CISSP ارزیابی و آزمون امنیتی(Security Assessment and Testing)

دامنه ششم از آزمون بین‌المللی CISSP با تمرکز بر ارزیابی و آزمون امنیتی به بررسی روش‌ها، تکنیک‌ها و ابزارهای مورد استفاده در سنجش کارایی و اثربخشی کنترل‌های امنیتی می‌پردازد. هدف این بخش، آموزش نحوه شناسایی آسیب‌پذیری‌ها، ارزیابی آن‌ها و بررسی وضعیت امنیتی سیستم‌ها به‌صورت مستمر و مستند است.

بخش اول: مفاهیم پایه ارزیابی امنیتی

1. **اعتبارسنجی(Validation)**
   - بررسی تطابق سیستم با نیازمندی‌ها و اهداف تعریف‌شده.
2. **راستی‌آزمایی(Verification)**
   - بررسی صحت پیاده‌سازی صحیح اجزای فنی.
3. **سطوح سخت‌گیری(Rigour Levels)**
   - از آزمون‌های ساده تا ارزیابی‌های عمیق و دقیق.
4. **انواع آزمون‌ها:**
   - آزمون واحد(Unit Testing)
   - آزمون رابط(Interface Testing)
   - آزمون یکپارچگی(Integration Testing)

- آزمون سیستم(System Testing)

بخش دوم: تکنیک‌ها و روش‌های آزمون

- **روش‌های دستی :** با دخالت انسانی
- **روش‌های خودکار :** استفاده از ابزارها و اسکریپت‌ها
- **آزمون ایستا (Static Testing)** بررسی کد بدون اجرا
- **آزمون پویا (Dynamic Testing)** بررسی در حین اجرای کد
- **آزمون Fuzzing & Mutation** تولید داده‌های غیرمنتظره برای بررسی رفتار سیستم

بخش سوم: انواع تکنیک‌های آزمون از دیدگاه دسترسی

- **آزمون سفید (White-box)** دسترسی کامل به کد
- **آزمون سیاه (Black-box)** بدون آگاهی قبلی
- **آزمون خاکستری (Gray-box)** دسترسی محدود به اطلاعات

انواع سناریوهای آزمون:

- مثبت(Positive)
- منفی(Negative)
- سوءاستفاده(Misuse Testing)

تحلیل‌های آزمونی:

- تحلیل جدول تصمیم(Decision Table)
- تحلیل حالت‌ها(State-Based Analysis)

- تحلیل مرزها(Boundary Value Analysis)
- بخش‌بندی معادل(Equivalence Partitioning)

بخش چهارم: آزمون‌های عملیاتی و عملکردی

- آزمون بازگشتی(Regression Testing)
- آزمون عملکرد واقعی(Real User Monitoring)
- آزمون مصنوعی(Synthetic Performance Monitoring)

بخش پنجم: نقش‌ها و مسئولیت‌ها در آزمون امنیتی

- مدیریت اجرایی(Executive Management)
- کمیته ممیزی(Audit Committee)

- مدیر امنیت اطلاعات(Security Officer)
- مدیر تطابق(Compliance Manager)
- ممیزان داخلی / خارجی(Internal / External Auditors)

بخش ششم: آسیب‌پذیری‌ها و تست نفوذ(Vulnerability & Pen Testing)

مراحل:

- شناسایی(Reconnaissance)
- شمارش(Enumeration)
- تحلیل آسیب‌پذیری‌ها(Vulnerability Analysis)
- بهره‌برداری(Exploitation)
- مستندسازی یافته‌ها

دیدگاه‌ها:

- داخلی(Internal)
- خارجی(External)

رویکردها:

- کور(Blind)
- دابل کور(Double-Blind)
- بدون دانش(Black-box)
- با دانش محدود(Gray-box)
- با دانش کامل(White-box)

انواع اسکن:

- دارای اعتبار(Credentialed)

- بدون اعتبار(Uncredentialed)

ابزارها:

- Banner Grabbing
- Fingerprinting

پروتکل‌ها و استانداردها:

- CVE
- CVSS
- SCAP

نتایج آزمون:

- خطای مثبت(False Positive)
- خطای منفی(False Negative)

بخش هفتم: ثبت و تحلیل لاگ‌ها(Log Review & SIEM)

- محدودسازی اندازه فایل لاگ
- بررسیTimestamp ، اررورها، تلاش برای تغییر یا رخنه
- سیستم‌های چرخه‌ای لاگ(Circular Overwrite)
- سطح برش(Clipping Levels)
- استفاده از NTP برای هماهنگی زمانی
- فرآیندهای لاگ:
  - جمع‌آوری(Collection)
  - نرمال‌سازی(Normalization)
  - تحلیل(Analysis)
  - نگه‌داری و حذف(Retention & Disposal)

ابزارهای SIEM

- Splunk
- IBM QRadar
- ELK Stack

منابع پیشنهادی برای یادگیری بیشتر:

- کتاب رسمیISC2 CISSP CBK
- Cybrary: Security Assessment & Testing
- دوره‌های Udemy و Pluralsight در مورد Penetration Testing وSIEM
- OWASP Testing Guide