مجموعه ۱۰۰ سؤال پرتکرار و به‌روز آزمون کتبی و مصاحبه حضوری افتا در گرایش "امن‌سازی و مقاوم‌سازی سامانه‌ها"

مجموعه ۱۰۰ سؤال پرتکرار و به‌روز آزمون کتبی و مصاحبه حضوری افتا در گرایش "امن‌سازی و مقاوم‌سازی سامانه‌ها" که به‌صورت استاندارد، پروژه‌محور و با پاسخ تشریحی ارائه شده که این سؤالات بر اساس تجربه ممیزی‌های واقعی افتا، سؤالات مصاحبه شرکت‌های ارزیاب و تطبیق با الزامات مرکز افتا تدوین شده‌اند.

ساختار سؤالات:

- **بخش A: مفاهیم و الزامات افتا (۱–۲۰)**
- **بخش B: امن‌سازی سیستم‌عامل و سرور (۲۱–۴۰)**
- **بخش C: امن‌سازی شبکه و ارتباطات (۴۱–۶۰)**
- **بخش D: مقاوم‌سازی سامانه‌ها و سرویس‌ها (۶۱–۸۰)**
- **بخش E: سناریوهای عملی، مصاحبه و پروژه‌محور (۸۱–۱۰۰)**

بخش A – مفاهیم پایه و الزامات افتا

۱- تفاوت «امن‌سازی» و «مقاوم‌سازی» سامانه‌ها چیست؟

پاسخ:

امن‌سازی تمرکز بر پیشگیری(Hardening) ، کاهش سطح حمله (دارد، در حالی که مقاوم‌سازی تمرکز بر تداوم سرویس، تحمل خطا و بازیابی پس از حمله (Resilience) دارد. افتا هر دو را الزام می‌داند.

۲-دامنه خدمات گرایش امن‌سازی و مقاوم‌سازی سامانه‌ها در افتا چیست؟

پاسخ:

سیستم‌عامل، سرورها، سرویس‌ها، دیتابیس، اپلیکیشن، شبکه، لاگ، بکاپ، IAM، Patch Management و DR.

۳-مستند اصلی مرجع ارزیابی افتا در این گرایش چیست؟

پاسخ:

- الزامات مرکز افتا
- دستورالعمل امن‌سازی سامانه‌ها

- استانداردهای بومی افتا + تطبیق باISO ۲۷۰۰۱ / NIST

۴- Hardening چیست؟

پاسخ:

فرآیند کاهش سطح حمله با حذف سرویس‌های غیرضروری، محدودسازی دسترسی‌ها، اعمال تنظیمات امن و کنترل پیکربندی.

۵- Secure Baseline چیست؟

پاسخ:

پیکربندی مرجع امن برای یک سامانه که مبنای استقرار و ممیزی قرار می‌گیرد) مثلاً.(CIS Benchmark

۶- Least Privilege چیست و چرا در افتا مهم است؟

پاسخ:

اعطای حداقل سطح دسترسی لازم؛ افتا روی این اصل در اکانت‌های ادمین بسیار حساس است.

۷- Defense in Depth چیست؟

پاسخ:

چندلایه‌سازی امنیتی (Network, Host, Application, Data) برای جلوگیری از شکست تک‌نقطه‌ای.

۸-تفاوت Vulnerability و Threat چیست؟

پاسخ:

Vulnerabilityضعف داخلی است؛ Threat عامل یا سناریوی بهره‌برداری از آن ضعف.

۹- Patch Managementدر افتا چه جایگاهی دارد؟

پاسخ:

الزامی؛ شامل شناسایی، ارزیابی، تست و اعمال وصله‌ها با مستندسازی.

۱۰-تفاوت Security Policy وSecurity Procedure ؟

پاسخ:

Policyسطح بالا و مدیریتی است؛ Procedure اجرایی و گام‌به‌گام

۱۱. مدل CIA چیست و چه جایگاهی در افتا دارد؟

پاسخ تشریحی:

مدل CIA سه رکن اصلی امنیت اطلاعات است:

- **Confidentiality (محرمانگی:** جلوگیری از دسترسی غیرمجاز به اطلاعات
- **Integrity (یکپارچگی:** جلوگیری از تغییر غیرمجاز داده
- **Availability (دسترس‌پذیری:** اطمینان از در دسترس بودن سرویس

در افتا:

- هر کنترل امنیتی باید حداقل یکی از این سه رکن را پوشش دهد
- تمرکز افتا صرفاً Confidentiality نیست؛ **Availability در زیرساخت‌های حیاتی بسیار مهم است**

دام مصاحبه: پاسخ‌هایی که فقط روی محرمانگی تمرکز می‌کنند.

۱۲- Risk Assessment چیست و چرا افتا آن را الزام می‌داند؟

پاسخ تشریحی:

Risk Assessment فرآیند شناسایی، تحلیل و اولویت‌بندی ریسک‌هاست بر اساس:

- دارایی (Asset)
- تهدید (Threat)
- آسیب‌پذیری (Vulnerability)
- اثر (Impact)
- احتمال (Likelihood)

افتا انتظار دارد:

- تصمیمات امنیتی **ریسک‌محور** باشند
- هر عدم انطباق، تحلیل ریسک و تصمیم مستند داشته باشد

جمله کلیدی مصاحبه:

"در افتا، امنیت مطلق نداریم؛ مدیریت ریسک داریم."

۱۳- Asset Classification چیست و چه نقشی در امن‌سازی دارد؟

پاسخ تشریحی:

طبقه‌بندی دارایی‌ها بر اساس ارزش و حساسیت، مانند:

- اطلاعات محرمانه
- سامانه حیاتی
- سرویس عمومی

در افتا:

- سطح امنیت باید متناسب با **طبقه دارایی** باشد
- همه سامانه‌ها الزام امنیتی یکسان ندارند

خطای رایج: اعمال کنترل‌های سنگین روی دارایی کم‌اهمیت یا برعکس.

۱۴- Secure Configuration چیست؟

پاسخ تشریحی:

پیکربندی امن سامانه‌ها بر اساس استانداردهای مرجع، نه تنظیمات پیش‌فرض.

شامل:

- غیرفعال‌سازی سرویس‌های غیرضروری
- تنظیمات امن OS ، DB، Network

- استفاده از Secure Baseline مثل (CIS)

در افتا:

- Default Configuration = ناامن
- Secure Configuration باید **مستند و قابل ممیزی** باشد

۱۵- Secure Baseline چیست و چه تفاوتی با Secure Configuration دارد؟

پاسخ تشریحی:

- **Secure Baseline:** وضعیت مرجع امن
- **Secure Configuration:** اجرای عملی آن Baseline

افتا از Baseline برای:

- استقرار
- ممیزی
- بررسی انحراف (Drift Detection)

استفاده می‌کند.

۱۶- Change Management چیست و چرا افتا روی آن حساس است؟

پاسخ تشریحی:

مدیریت تغییرات برای کنترل ریسک ناشی از تغییرات فنی.

الزامات افتا:

- ثبت درخواست تغییر
- ارزیابی اثر امنیتی

- تأیید
- برنامه بازگشت(Rollback)

نکته افتایی:

بسیاری از حوادث امنیتی، نتیجه تغییر بدون کنترل هستند.

۱۷- اگر تغییری بدون Change Management انجام شود چه ریسکی دارد؟

پاسخ تشریحی:

- ایجاد آسیب‌پذیری جدید
- از کار افتادن کنترل‌های امنیتی
- عدم امکان ردیابی حادثه

در افتا، تغییر بدون مستند = **عدم انطباق جدی**.

۱۸- Audit Trail چیست؟

پاسخ تشریحی:

ثبت زنجیره‌ای و غیرقابل‌انکار فعالیت‌ها شامل:

- چه کسی
- چه زمانی
- چه کاری انجام داده

Audit Trailبرای:

- Incident Response
- Forensic
- پاسخ‌گویی حقوقی

الزامی است.

۱۹-تفاوت Audit Trail و Log معمولی چیست؟

پاسخ تشریحی:

Audit Trail	Log
ثبت مسئولیت	ثبت رویداد
باید محافظت شود	ممکن است پاک شود
حقوقی–امنیتی	عملیاتی

افتا Audit Trail بدون محافظت را نمی‌پذیرد.

۲۰-الزامات افتا برای Audit Trail چیست؟

پاسخ تشریحی:

- Centralized Logging
- محافظت در برابر حذف و تغییر
- Time Sync
- نگهداری طبق سیاست
- دسترسی محدود به لاگ‌ها

جمله طلایی مصاحبه:

"سیستمی که لاگ ندارد، از نظر افتا وجود ندارد."

جمع‌بندی سریع سؤالات ۱۱–۲۰

- همه‌چیز از **دارایی** شروع می‌شود
- تصمیم‌ها باید **ریسک‌محور و مستند** باشند
- تنظیمات پیش‌فرض دشمن امنیت هستند

- تغییر کنترل‌نشده = حادثه امنیتی
- لاگ و Audit Trail ستون پاسخ‌گویی افتاست

بخش B – امن‌سازی سیستم‌عامل و سرور

۲۱-اولین اقدام امن‌سازی یک سرور تازه نصب‌شده چیست؟

پاسخ:

اعمال Secure Baseline، تغییر Credential پیش‌فرض، Patch اولیه.

۲۲-چرا حذف سرویس‌های غیرضروری مهم است؟

پاسخ:

هر سرویس فعال، یک Attack Surface بالقوه است.

۲۳-نقش SELinux / AppArmor در افتا چیست؟

پاسخ:

کنترل دسترسی اجباری (MAC) برای محدودسازی رفتار فرآیندها.

۲۴-تفاوت Hardening ویندوز و لینوکس؟

پاسخ:

ویندوز: GPO، Registry، Local Policy

لینوکس: Sysctl، PAM، Permissions، Services

۲۵- SSH Hardening شامل چه مواردی است؟

پاسخ:

- Disable Root Login
- Key-based Auth
- محدودسازی IP
- تغییر پورت (در صورت توجیه)

۲۶-چرا افتا روی Time Sync حساس است؟

پاسخ:

برای اعتبار لاگ‌ها و Incident Response NTP امن.

۲۷- نقش File Integrity Monitoring چیست؟

پاسخ:

تشخیص تغییرات غیرمجاز فایل‌های حیاتی.

۲۸- Secure Boot چیست؟

پاسخ:

جلوگیری از بوت شدن کدهای غیرمجاز.

۲۹-اهمیت لاگ سطح OS در افتا؟

پاسخ:

الزامی برای Trace ، Forensic و پاسخ به حادثه.

۳۰-چگونه دسترسی sudo امن می‌شود؟

پاسخ:

Role-based sudo، ثبت لاگ، بدون NOPASSWD.

۳۱- Hardening پایگاه داده (Database Hardening) شامل چه اقداماتی است؟

پاسخ تشریحی:

Hardening دیتابیس به معنای کاهش سطح حمله و جلوگیری از سوءاستفاده از داده‌ها و سرویس DB است.

اقدامات کلیدی:

- *حذف یا غیرفعال‌سازی حساب‌های پیش‌فرض (default users)*
- *اعمال **Role-Based Access Control (RBAC)***
- *محدودسازی دسترسی شبکه‌ای به DB (Bind به IP خاص)*
- *رمزنگاری داده در حالت Rest و Transit*

- فعال‌سازی لاگ‌های امنیتی (Audit Log)
- منظم موتور دیتابیس Patch
- غیرفعال‌سازی Stored Procedure های غیرضروری

نکته مصاحبه‌ای افتا:

"دیتابیس نباید مستقیماً در معرض شبکه کاربر یا اینترنت باشد."

۳۲- Secure Service Account چیست و چرا افتا روی آن حساس است؟

پاسخ تشریحی:

Service Account حسابی است که سرویس‌ها با آن اجرا می‌شوند.

الزامات افتا:

- حداقل سطح دسترسی (Least Privilege)
- عدم استفاده از حساب‌های اشتراکی
- عدم Login تعاملی (No Interactive Login)
- تغییر دوره‌ای رمز عبور یا استفاده از Secret Manager
- ثبت لاگ استفاده

خطای رایج: اجرای سرویس‌ها با root یا Administrator.

۳۳- Password Policy مورد قبول افتا چه ویژگی‌هایی دارد؟

پاسخ تشریحی:

Password Policy باید شامل:

- حداقل طول (حداقل ۱۲ کاراکتر)
- پیچیدگی (حروف بزرگ، کوچک، عدد، نماد)
- تاریخ انقضا مشخص

- عدم استفاده مجدد از رمزهای قبلی
- Lockoutپس از تلاش ناموفق
- ذخیره به‌صورت Hash شده نه (Plain)

افتا استفاده از **Passphrase** را ترجیح می‌دهد.

۳۴- MFA چیست و در چه لایه‌هایی باید پیاده‌سازی شود؟

پاسخ تشریحی:

Multi-Factor Authenticationترکیب حداقل دو عامل از:

- دانستنی (Password)
- داشتنی (Token)
- ذاتی (Biometric)

در افتا، MFA **الزامی** است برای:

- دسترسی ادمین
- دسترسی راه دور (VPN)
- پنل‌های مدیریتی حیاتی

۳۵- Cron Security چیست و چه تهدیدی را پوشش می‌دهد؟

پاسخ تشریحی:

Cron Jobها می‌توانند محل اجرای کد مخرب باشند. اقدامات امن‌سازی:

- محدودسازی دسترسی به crontab
- بررسی دوره‌ای jobها
- اجرای cron با کاربر محدود

- ثبت لاگ اجرای cron
- جلوگیری از world-writable script ها

سؤال پرتکرار مصاحبه:

"چگونه بدافزار از cron استفاده می‌کند؟"

بدافزارها از **Cron** به‌عنوان مکانیزم **پایداری (Persistence)** و **اجرای دوره‌ای کد مخرب** استفاده می‌کنند تا حتی پس از ریبوت یا حذف موقت، دوباره فعال شوند.

۳۶- Resource Limitation چیست و چه نقشی در مقاوم‌سازی دارد؟

پاسخ تشریحی:

محدودسازی منابع برای جلوگیری از DoS داخلی یا سوءاستفاده:

- CPU Limit
- Memory Limit
- Disk Quota
- Process Limit

در لینوکس:

- ulimit
- cgroups

هدف: جلوگیری از سقوط کل سیستم به‌دلیل یک فرآیند.

۳۷- تفاوت Antivirus و EDR در نگاه افتا چیست؟

پاسخ تشریحی:

EDR	Antivirus
تحلیل رفتاری	تشخیص امضامحور
Responseفعال	واکنش محدود
مناسب APT	مناسب تهدیدات ساده

افتا در سامانه‌های حیاتی، **EDRرا ترجیح می‌دهد.**

۳۸- CIS Benchmark چیست و چه جایگاهی در افتا دارد؟

پاسخ تشریحی:

CIS Benchmarkمجموعه پیکربندی‌های امن مرجع برای:

- OS
- DB
- Network Devices

در افتا:

- به‌عنوان **Baselineامن‌سازی قابل استناد**
- قابل استفاده در ممیزی و دفاع فنی

الزام: مستندسازی انطباق یا عدم انطباق با CIS.

۳۹- Bastion Host چیست و چه زمانی استفاده می‌شود؟

پاسخ تشریحی:

Bastion Hostسرور واسط امن برای دسترسی مدیریتی است:

- تنها نقطه ورود ادمین‌ها

- *لاگ کامل دسترسی*
- *MFA*
- *محدودسازی IP*
- *عدم اجرای سرویس غیرمدیریتی*

در افتا، *Bastion راهکار استاندارد مدیریت دسترسی است .*

۴۰- *رابطه Hardening و Compliance در افتا چیست؟*

پاسخ تشریحی:

- *Hardening = اجرای فنی واقعی*
- *Compliance = انطباق مستند با الزامات*

افتا بدون اجرای عملی Hardening ، ***Compliance را نمی‌پذیرد .***

بخش C – امن‌سازی شبکه و ارتباطات

۴۱- Segmentation .چیست و چرا افتا الزام می‌کند؟

پاسخ:

تفکیک شبکه برای جلوگیری از حرکت جانبی مهاجم.

۴۲- Zero Trust چیست؟

پاسخ:

عدم اعتماد پیش‌فرض حتی به کاربران داخلی.

۴۳-تفاوت Firewall وIPS ؟

پاسخ:

Firewallمبتنی برRule ، IPSمبتنی بر الگوی حمله.

۴۴- Secure Protocol چیست؟ مثال بزنید.

پاسخ:

TLS, HTTPS, SFTPبه‌جای نسخه‌های Plain.

۴۵-چرا SNMP v۱/v۲ ناامن است؟

پاسخ:

عدم رمزنگاری و احراز هویت قوی.

۴۶- VPN مورد قبول افتا چه ویژگی‌هایی دارد؟

پاسخ:

رمزنگاری قوی، MFA، لاگ، محدودسازی دسترسی.

۴۷- DMZ چیست؟

پاسخ:

ناحیه واسط بین شبکه داخلی و بیرونی.

۴۸- چرا افتا روی DNS Security حساس است؟

پاسخ:

DNS Attack = اختلال گسترده سرویس.

۴۹- Network Hardening شامل چه مواردی است؟

پاسخ:

ACL، Rate Limit، Disable Unused Ports.

۵۰- Role NAC در مقاوم‌سازی؟

پاسخ:

کنترل دسترسی تجهیزات به شبکه.

بخش – D مقاوم‌سازی سامانه‌ها

۶۱- Resilience چیست؟

پاسخ:

توان ادامه سرویس‌دهی در شرایط حمله یا خرابی.

۶۲- تفاوت Backup وDR ؟

پاسخ:

Backupداده؛ DR تداوم کل سرویس.

۶۳- RTO و RPO چیست؟

پاسخ:

RTO:زمان بازیابی

RPO:میزان داده قابل‌قبول از دست رفته

۶۴- HA چیست؟

پاسخ:

High Availabilityبا حذف Single Point of Failure.

۶۵- Load Balancerچه نقشی دارد؟

پاسخ:

توزیع بار و افزایش دسترس‌پذیری.

۶۶- Failover چیست؟

پاسخ:

انتقال خودکار سرویس به نود جایگزین.

۶۷- Immutable Backupچیست؟

پاسخ:

بکاپ غیرقابل تغییر برای مقابله با Ransomware.

۶۸- چرا تست DR مهم است؟

پاسخ:

DRبدون تست، صرفاً یک سند است.

۶۹- Geo-Redundancy چیست؟

پاسخ:

توزیع سرویس در مکان‌های جغرافیایی مختلف.

۷۰- Chaos Engineering چه کمکی می‌کند؟

پاسخ:

آزمون تحمل سامانه در شرایط بحرانی. حتماً.

۷۱- Monitoring چیست و چه تفاوتی با Logging دارد؟

پاسخ تشریحی:

Monitoringپایش بلادرنگ وضعیت سامانه(CPU ، RAM، Availability، Latency)است، در حالی که Logging ثبت رویدادها برای تحلیل، Forensicو Incident Response است.

در افتا، هر دو الزامی و مکمل هستند.

دام سؤال: پاسخ‌هایی که Monitoring را فقط نمودار می‌دانند.

۷۲-حداقل الزامات Monitoring مورد قبول افتا چیست؟

پاسخ تشریحی:

- پایش Availability سرویس‌های حیاتی
- پایش مصرف منابع
- Alertآستانه‌ای(Threshold-based)
- ثبت و نگهداری سوابق پایش
- اتصال به فرآیندIncident Response

نکته افتایی: مانیتورینگ بدونAlert ، صرفاً گزارش‌گیری است.

۷۳- Auto-Scaling چیست و چه نقشی در مقاوم‌سازی دارد؟

پاسخ تشریحی:

Auto-Scalingافزایش یا کاهش خودکار منابع متناسب با بار است.

در افتا:

- کاهش ریسکOverload
- افزایش دسترس‌پذیری
- کمک به مقابله با حملات حجمی محدود

دام سؤال Auto-Scaling :جایگزین امنیت نیست.

۷۴- آیا Auto-Scaling می‌تواند خطرناک باشد؟

پاسخ تشریحی:

بله. در صورت عدم کنترل:

- افزایش هزینه غیرقابل پیش‌بینی
- تشدید حملات مصرف منابع

راهکار افتایی:

- Rate Limit
- سقف منابع
- Alertمالی و فنی

۷۵- Circuit Breaker چیست و چه کاربردی دارد؟

پاسخ تشریحی:

الگویی برای جلوگیری از شکست زنجیره‌ای سرویس‌ها.

در صورت بروز خطای مکرر، ارتباط موقتاً قطع می‌شود تا سامانه پایدار بماند.

کاربرد مهم در معماری Microservices.

۷۶-چه زمانی Circuit Breaker فعال می‌شود؟

پاسخ تشریحی:

- افزایش نرخ خطا
- Timeoutمکرر
- عدم پاسخ سرویس وابسته

افتا این الگو را مصداق «مقاوم‌سازی هوشمند» می‌داند.

۷۷- Incident Playbook چیست؟

پاسخ تشریحی:

سند عملیاتی شامل:

- نوع حادثه
- مسئول اقدام
- گام‌های پاسخ
- ابزارها
- مسیر Escalation

Playbookباید **تست‌شده و تمرین‌شده** باشد.

۷۸- Business Continuity (BC)چیست و چه تفاوتی با DR دارد؟

پاسخ تشریحی:

BCتضمین تداوم فرآیندهای حیاتی کسب‌وکار است؛

DRزیرمجموعه فنی BC برای بازیابی IT است.

افتا نگاه فرآیندی دارد، نه فقط فنی.

۷۹- Capacity Planning چیست و چرا افتا آن را بررسی می‌کند؟

پاسخ تشریحی:

برنامه‌ریزی ظرفیت برای پاسخ‌گویی به رشد بار و بحران‌ها.

شامل:

- تحلیل روند مصرف
- پیش‌بینی رشد
- تعریف آستانه هشدار

نبود = Capacity Planning ریسک خاموشی.

۸۰- چگونه Capacity Planning به امنیت کمک می‌کند؟

پاسخ تشریحی:

- کاهش اثر حملات مصرف منابع
- جلوگیری از Fail ناگهانی
- تصمیم‌گیری آگاهانه برایAuto-Scaling

افتا ظرفیت ناکافی را **ریسک امنیتی** تلقی می‌کند.

جمع‌بندی طلایی سؤالات ۷۱–۸۰ برای آزمون و مصاحبه افتا

- مقاوم‌سازی فقط بکاپ نیست
- پایش + واکنش = امنیت عملیاتی

- هر ابزار باید به **فرآیند تصمیم‌گیری** متصل باشد
- مستندسازی + تست = امتیاز قبولی

بخش – E سناریوهای مصاحبه حضوری (بسیار مهم)

۸۱- اگر سرور حیاتی Patch نشود چه می‌کنید؟

پاسخ:

Risk Acceptanceمستند + کنترل جبرانی.

۸۲- سناریوی نفوذ از طریق SSH را تحلیل کنید.

پاسخ:

Credential Leak → Lateral Movement → Privilege Escalation.

۸۳-چگونه Hardening را مستند می‌کنید؟

پاسخ:

Before/After Config. ،Baseline ،Checklist

۸۴-افتا در مصاحبه بیشتر دنبال چیست؟

پاسخ:

تجربه عملی، درک ریسک، تصمیم مهندسی.

۸۵-اگر کارفرما خلاف الزامات افتا بخواهد؟

پاسخ:

اعلام ریسک، مستندسازی، عدم پذیرش شفاهی.

۸۶- Secure Deployment Pipeline چیست؟

پاسخ:

CI/CDهمراه با کنترل امنیت.

۸۷- چگونه تغییرات را کنترل می‌کنید؟

پاسخ:

Change Management + Rollback Plan.

۸۸-فرق Hardening دستی و اتوماتیک؟

پاسخ:

اتوماتیک پایدارتر و قابل ممیزی.

۸۹-سناریوی قطع دیتاسنتر اصلی؟

پاسخ:

فعال‌سازی DR Site طبق BCP.

۹۰-چگونه اثربخشی امن‌سازی را می‌سنجید؟

پاسخ:

Vulnerability Scan + Audit.

۹۱-ابزارهای رایج Hardening ؟

پاسخ:

Ansible، CIS-CAT، OpenSCAP.

۹۲-نقش SIEM در این گرایش؟

پاسخ:

تشخیص، همبستگی و پاسخ به حادثه.

۹۳-آیا رمزنگاری همیشه کافی است؟

پاسخ:

خیر؛ Key Management حیاتی است.

۹۴-تفاوت Compliance و Security ؟

پاسخ:

Complianceحداقل الزام؛ Security هدف واقعی.

۹۵-اگر لاگ‌ها حذف شوند؟

پاسخ:

Central Logging + WORM Storage.

۹۶-خطای رایج شرکت‌های افتایی؟

پاسخ:

تمرکز صرف بر سند، نه اجرا.

۹۷-چگونه دانش خود را به‌روز نگه می‌دارید؟

پاسخ:

Advisory، CVE، تمرین عملی.

۹۸-مهم‌ترین اصل در افتا؟

پاسخ:

مسئولیت‌پذیری و مستندسازی.

۹۹- تفاوت Auditor و Implementer ؟

پاسخ:

Auditorارزیاب؛ Implementer مجری.

۱۰۰- چرا شما را باید تأیید کنیم؟

پاسخ:

ترکیب دانش، تجربه عملی و درک ریسک ملی.

با آرزوی موفقیت برای تیم پر تلاش بدررایان خوزستان

مجموعه ۱۰۰ سؤال پرتکرار و به‌روز آزمون کتبی و مصاحبه حضوری افتا در گرایش "امن‌سازی و مقاوم‌سازی سامانه‌ها"

خلاصه‌ی طلایی شب امتحان افتا

برای گرایش امن‌سازی و مقاوم‌سازی سامانه‌ها به‌گونه‌ای طراحی شده که در ۳۰ تا ۴۵ دقیقه قابل مرور باشد و دقیقاً روی نقاط سؤال‌خیز آزمون کتبی و مصاحبه حضوری افتا تمرکز دارد.

۱-مفاهیم کلیدی که حتماً می‌پرسند

امن‌سازی:(Hardening)

کاهش سطح حمله با حذف سرویس‌های غیرضروری، محدودسازی دسترسی‌ها، .Secure Configuration

مقاوم‌سازی:(Resilience)

تداوم سرویس در شرایط حمله، خطا یا بحران(HA) ، DR، .Auto-Scaling

نکته امتحانی:

افتا هرگز یکی را بدون دیگری نمی‌پذیرد.

۲-اصول طلایی افتا (حفظی + مفهومی)

- Least Privilege
- Defense in Depth
- Secure by Design
- مستندسازی + شواهد فنی
- تصمیم ریسک‌محور (نه مطلق)

۳- Hardening (سیستم‌عامل (خیلی پرتکرار)

باید بلد باشید بگویید:

- Secure Baselineترجیحاً(CIS)
- حذفDefault Account
- Patch Management
- SSH Hardening (Key, MFA, IP Restrict)

- لاگ و Time Sync
- عدم استفاده از root / Administrator

دام رایج:

"تغییر پورت = SSH امنیت" ❌

۴- Hardening (دیتابیس -سؤال دام‌دار)

- DBهرگز مستقیم روی اینترنت ❌
- RBAC
- Encrypt (Rest + Transit)
- Audit Log
- محدودسازیNetwork Access
- Patch DB Engine

۵) Service Account وPassword Policy

Service Account:

- حداقل دسترسی
- بدون Login تعاملی
- لاگ‌دار
- بدون استفاده مشترک

Password Policyافتایی:

- حداقل ۱۲ کاراکتر
- Expire
- Lockout

- Hash
- ترجیحPassphrase

۶- MFA (حتماً می‌پرسند)

MFAالزامی است برای:

- ادمین‌ها
- VPN
- Bastion
- پنل‌های مدیریتی

MFA = Password +عامل دوم(Token / App)

۷- Bastion Host (نقطه طلایی مصاحبه)

- تنها نقطه ورود مدیریتی
- MFA
- لاگ کامل
- بدون سرویس جانبی
- محدودسازیIP

جمله نجات‌بخش مصاحبه:

"دسترسی ادمین بدون Bastion ریسک ملی است."

۸- Monitoring (و) Logging فرق را دقیق بگویید

Monitoring:وضعیت لحظه‌ای

Logging:ثبت رویداد برایForensic

افتایی:

Monitoringبدون = Alert بی‌ارزش

۹-EDR (Antivirusو ابزارها)

- Antivirus → امضامحور
- EDR → رفتاریResponse +
- ابزار بدون معماری = امنیت نمایشی ✗

۱۰- (مقاوم‌سازی – (Resilience خیلی مهم

باید بلد باشید:

- Backup ≠ DR
- RTO / RPO
- HA
- Failover
- Immutable Backup
- تستDR

۱۱- Auto-Scaling وCircuit Breaker

Auto-Scaling:

کمک به تحمل بار، نه جایگزین امنیت

Circuit Breaker:

قطع موقت ارتباط برای جلوگیری از Fail زنجیره‌ای

۱۲-(Incident Playbook)

باید شامل:

- نوع حادثه

- مسئول
- مراحل اقدام
- Escalation
- تست‌شده باشد

۱۳- Business Continuity و Capacity Planning

BC: تداوم فرآیند

DR: بازیابی IT

Capacity Planning:

- پیش‌بینی رشد
- آستانه هشدار
- جلوگیری از DoS داخلی

۱۴-سؤالات نهایی مصاحبه (جواب آماده)

سؤال : چرا شما؟

جواب:

چون تصمیمات من ریسک‌محور، مستند، اجرایی و منطبق با الزامات افتا است؛ نه صرفاً تئوریک یا ابزارمحور.

۱۵- ۵ خط قرمز افتا (حتماً حفظ کنید)

۱. سند بدون اجرا ❌

۲. ابزار بدون فرآیند ❌

۳. ادمین بدون لاگ ❌

٤. دیتابیس در اینترنت ❌

۵. تصمیم شفاهی بدون مستند ❌

توصیه نهایی شب امتحان

- جواب کوتاه + مهندسی
- اشاره به **ریسک و مستند** در هر پاسخ
- از جواب‌های مطلق پرهیز کن
- بگو «در صورت اجبار» → Risk Acceptance

با آرزوی موفقیت برای تیم پر تلاش بدررایان خوزستان