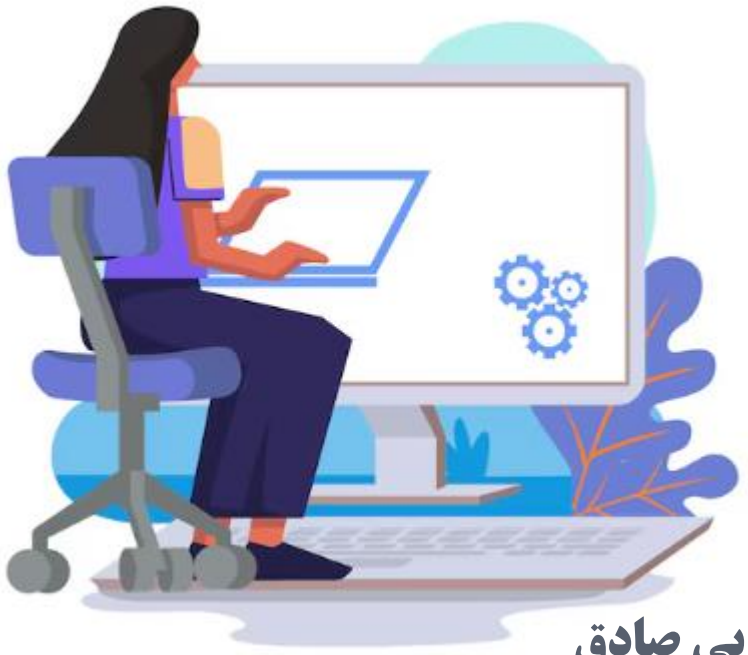
آشنایی با صنعت کامپیوتر

اسلاید سوم

(شروعی موفق در دنیای فناوری: آشنایی با مهارت‌های فنی در صنعت کامپیوتر)

امنیت سایبری – پایگاه داده



درس
آشنایی با صنعت کامپیوتر

۳

محمد سعید صفایی صادق

۱۴۰۴

۴- امنیت سایبری

۱-۴: تعریف امنیت سایبری:

امنیت سایبری به مجموعه‌ای از تکنیک‌ها، روش‌ها و فرآیندها اطلاق می‌شود که برای حفاظت از سیستم‌ها و داده‌ها در برابر دسترسی‌های غیرمجاز، خرابکاری، تغییرات ناخواسته و تهدیدات خارجی یا داخلی طراحی شده‌اند.

این شامل استفاده از ابزارهای مختلف امنیتی مانند فایروال‌ها، سیستم‌های شناسایی نفوذ IDS و رمزنگاری می‌شود.

هدف اصلی امنیت سایبری حفظ محرمانگی، تمامیت و دسترسی به اطلاعات و سیستم‌ها است.

۱-۴: ویژگی های مهم امنیت سایبری:

۱- محرمانگی Confidentiality : حفاظت از داده‌ها از دسترسی غیرمجاز و اطمینان از این که اطلاعات تنها در اختیار افراد مجاز قرار دارد.

۲- تمامیت Integrity : اطمینان از این که داده‌ها و سیستم‌ها در برابر تغییرات غیرمجاز محافظت شده‌اند و فقط افراد مجاز قادر به تغییر آن‌ها هستند.

۳- دسترس‌پذیری Availability : اطمینان از اینکه سیستم‌ها و داده‌ها در هر زمان در دسترس کاربران مجاز قرار دارند.

۱-۴: ویژگی های مهم امنیت سایبری:

نکته : این سه باید در کنار هم رعایت شود، فقدان هریک یعنی نا امنی

۱-۴: برخی انواع تهدیدات سایبری:

۱- **ویروس‌ها و بدافزارها**: برنامه‌هایی که به طور مخفیانه وارد سیستم می‌شوند و هدفشان خرابکاری، دزدی داده یا جاسوسی است.

۲- **حملات فیشینگ**: حملاتی که از طریق ایمیل‌ها یا وب‌سایت‌های جعلی برای دزدیدن اطلاعات حساس کاربران (مانند رمز عبور) طراحی شده‌اند.

۳- **حملات DDoS (Distributed Denial of Service)**:
حملاتی که هدفشان از کار انداختن یک سیستم یا سرویس با ارسال حجم بالای درخواست‌ها به آن سیستم است.

۴- **حملات MITM (Man-In-The-Middle)**: حملاتی که در آن یک مهاجم به طور مخفیانه ارتباطات بین دو طرف را رهگیری و ممکن است تغییر دهد.

۱-۴: ابزار های امنیت سایبری:

۱- **فایروال‌ها Firewalls :** ابزارهایی که به منظور فیلتر کردن ترافیک ورودی و خروجی شبکه برای جلوگیری از دسترسی غیرمجاز و حملات استفاده می‌شوند.

۲- **سیستم‌های شناسایی نفوذ IDS/IPS :** سیستم‌هایی که به طور فعال ترافیک شبکه را برای شناسایی و جلوگیری از حملات بررسی می‌کنند.

۳- **رمزنگاری Encryption :** فرآیند تبدیل داده‌ها به یک فرمت غیرقابل خواندن برای جلوگیری از دسترسی غیرمجاز.

۴- **VPN شبکه خصوصی مجازی:** ابزاری که ارتباطات اینترنتی را از طریق تونل‌های امن رمزنگاری‌شده برقرار می‌کند.

۱-۴: مهارت های کلیدی امنیت سایبری:

۱- **شناسایی و مدیریت تهدیدات**: توانایی شناسایی تهدیدات و آسیب‌پذیری‌های سیستم و شبکه و مدیریت ریسک‌ها.

۲- **رمزنگاری و امنیت داده‌ها**: تسلط بر روش‌های رمزنگاری و حفاظت از اطلاعات حساس.

۳- **امنیت شبکه**: توانایی ایجاد و پیکربندی فایروال‌ها، IDS/IPSو سایر تجهیزات امنیتی شبکه.

۴- **مدیریت دسترسی و احراز هویت**: طراحی سیستم‌های احراز هویت و مدیریت دسترسی کاربران به منابع حساس.

۵- **تحلیل و پاسخ به حملات**: توانایی شناسایی حملات در حال وقوع، تحلیل آن‌ها و پاسخ مناسب برای محدود کردن آسیب‌ها.

۱-۴: فناوری ها و ابزار نرم افزاری امنیت سایبری:

۱- **Kali Linux** : سیستم‌عاملی محبوب برای تست نفوذ و ارزیابی امنیت.

۲- **Wireshark** : ابزار تحلیل بسته‌های داده در شبکه برای شناسایی تهدیدات.

۳- **Metasploit** : ابزاری برای شبیه‌سازی حملات و ارزیابی آسیب‌پذیری‌ها.

۴- **Splunk** : پلتفرمی برای نظارت بر داده‌های امنیتی و شناسایی تهدیدات.

۱-۴: دوره های مبتدی و پایه امنیت سایبری:

۱- CompTIA Security+ :

یکی از معتبرترین دوره‌های مبتدی در زمینه امنیت سایبری است که مفاهیم پایه امنیت شبکه، رمزنگاری، تهدیدات و آسیب‌پذیری‌ها، و مدیریت ریسک را پوشش می‌دهد.

مخاطبین: مبتدیان در امنیت سایبری، کسانی که قصد دارند وارد حوزه امنیت شوند.

۲- Cisco CCNA Security :

این دوره به بررسی اصول امنیت شبکه، پیکربندی و مدیریت فایروال‌ها، VPNها، و شناسایی تهدیدات شبکه می‌پردازد.

مخاطبین: افرادی که می‌خواهند در زمینه امنیت شبکه تخصص پیدا کنند.

۱-۴: دوره های پیشرفته امنیت سایبری:

۱- Certified Information Systems Security Professional (CISSP):

این گواهی‌نامه برای کسانی است که می‌خواهند در مدیریت امنیت سازمان‌ها و سیستم‌های اطلاعاتی فعالیت کنند.

CISSP مفاهیم پیشرفته‌ای مانند مدیریت امنیت، رمزنگاری، و سیاست‌های امنیتی را پوشش می‌دهد.

۲- Certified Ethical Hacker (CEH):

این دوره به یادگیری روش‌های تست نفوذ و شبیه‌سازی حملات برای شناسایی آسیب‌پذیری‌ها در سیستم‌ها می‌پردازد.

این دوره به طور خاص برای افرادی است که می‌خواهند در زمینه تست نفوذ Penetration Testing فعالیت کنند.

۱-۴: دوره های پیشرفته امنیت سایبری:

۳- Certified Information Security Manager (CISM):

این گواهی‌نامه بر مدیریت امنیت اطلاعات تمرکز دارد و برای افرادی مناسب است که در مدیریت امنیت سازمان‌ها فعالیت می‌کنند.

مخاطبین: مدیران امنیت اطلاعات و کسانی که مسئولیت نظارت و مدیریت امنیت را بر عهده دارند.

۱-۴: دوره های خاص امنیت سایبری:

۱- Kali Linux :

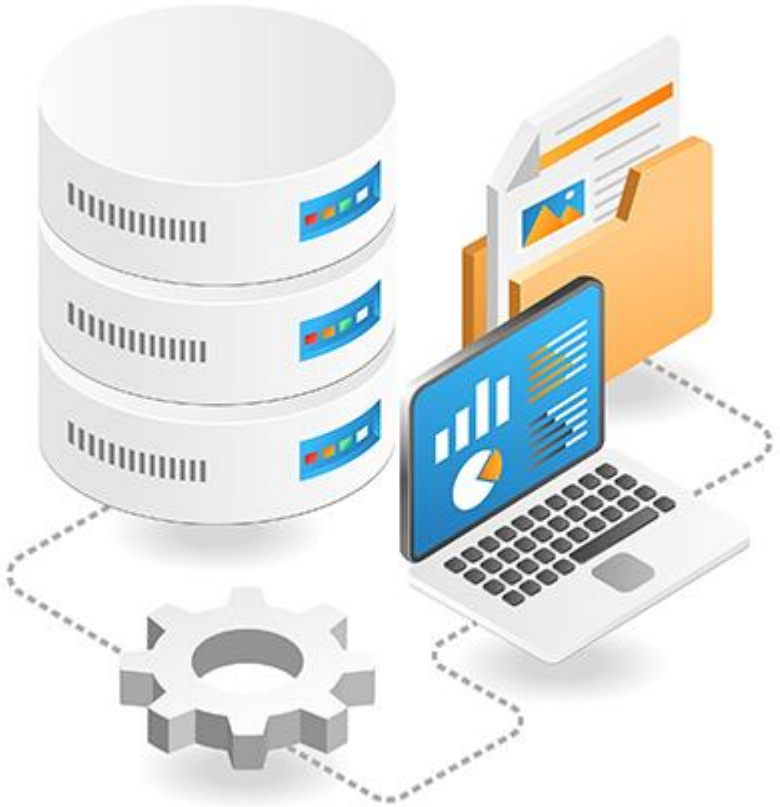
Kali Linux یک توزیع لینوکس است که به طور ویژه برای تست نفوذ و تحلیل امنیتی طراحی شده است.

دوره‌های مختلفی برای یادگیری نحوه استفاده از این ابزار و شبیه‌سازی حملات سایبری وجود دارد.

۲- Wireshark :

Wireshark یکی از ابزارهای محبوب برای تحلیل شبکه و شناسایی تهدیدات است.

دوره‌هایی برای یادگیری نحوه استفاده از این ابزار برای نظارت بر ترافیک شبکه و شناسایی حملات مختلف موجود است.



۵– پایگاه داده

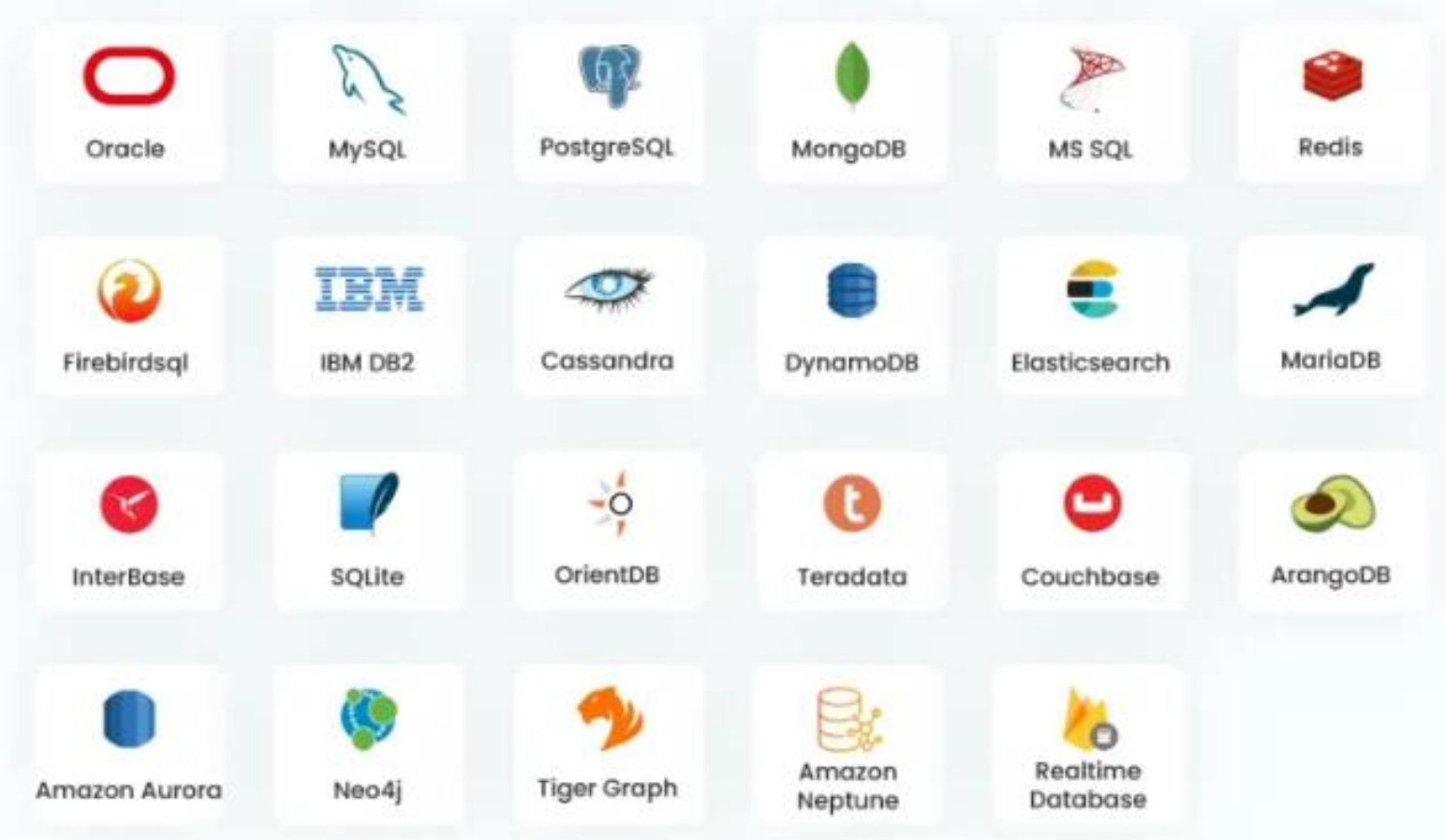
۱-۵: تعریف طراحی و پیاده‌سازی پایگاه داده:

طراحی پایگاه داده یعنی مشخص کردن ساختار داده‌ها (جداول، فیلدها، ارتباط‌ها و قوانین) به شکلی که داده‌ها منظم، قابل توسعه و بدون تناقض ذخیره شوند.

پیاده‌سازی پایگاه داده یعنی ساخت عملی این طراحی در یک سیستم مدیریت پایگاه داده DBMS مثل MySQL، PostgreSQL، SQL Server، Oracle، MongoDB و ...

و آماده‌سازی آن برای استفاده در برنامه.

۱-۵: تعریف طراحی و پیاده‌سازی پایگاه داده:



۱-۵: ویژگی‌های مهم پایگاه داده:

۱- دقت و یکپارچگی داده‌ها Data Integrity : جلوگیری از ورود داده‌های اشتباه یا ناسازگار با استفاده از کلیدها و محدودیت‌ها Constraints .

۲- کارایی Performance : طراحی درست برای سرعت بالای جستجو و پردازش داده‌ها (ایندکس، بهینه‌سازی کوئری).

۳- مقیاس‌پذیری Scalability : قابلیت رشد سیستم با افزایش کاربران و حجم داده.

۴- امنیت Security : تعیین سطح دسترسی کاربران، رمزگذاری، و جلوگیری از نشت اطلاعات.

۵- پایداری و بازیابی Reliability & Recovery : بکاپ‌گیری و امکان بازیابی اطلاعات در صورت خرابی یا خطا.

۱-۵: انواع پایگاه داده:

۱- **رابطه‌ای Relational / SQL :** داده‌ها در قالب جدول و رابطه ذخیره می‌شوند (مثل MySQL, PostgreSQL, SQL Server).

۲- **غیررابطه‌ای NoSQL :** برای داده‌های بزرگ یا ساختارهای انعطاف‌پذیر (مثل MongoDB, Redis, Cassandra .

۳- **ستونی Columnar :** مناسب تحلیل داده و گزارش‌گیری سنگین (مثل ClickHouse, BigQuery .

۴- **گراف Graph Database :** مناسب ارتباط‌های پیچیده مثل شبکه‌های اجتماعی مثل Neo4j .

۱-۵: مهارت‌های کلیدی برای کار با پایگاه داده:

۱- **SQL و کوئری‌نویسی**: SELECT، JOIN، GROUP BY، Subqueryو ...

۲- **طراحی ساختار جداول**: انتخاب نوع داده مناسب، طراحی درست ارتباط‌ها و Constraints.

۳- **بهینه‌سازی کوئری Query Optimization** : تحلیل کندی‌ها، استفاده از ایندکس و تنظیمات مناسب.

۴- **مدیریت تراکنش‌ها Transactions** : مفهوم ACID، جلوگیری از خطا در عملیات مالی یا حساس.

۵- **مدیریت و نگهداری Maintenance** : بکاپ، رستور، مانیتورینگ، Migrationو نسخه‌بندی.

۱-۵: دوره های آموزشی پایگاه داده:

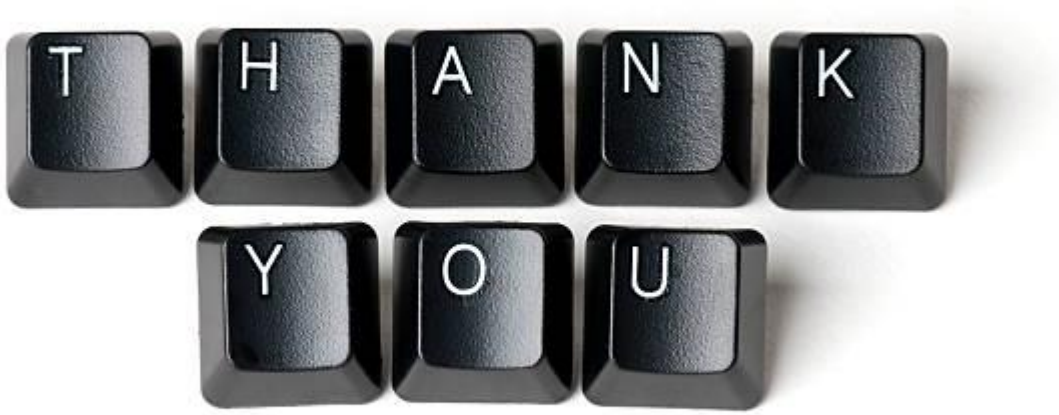
۱- **Microsoft SQL Server Certification :** دوره برای یادگیری مدیریت پایگاه داده‌های SQL Server از مایکروسافت.

۲- **MySQL Database Administration :** دوره‌ای برای مدیریت پایگاه داده MySQLو پیکربندی آن.

۳- **Udemy Database Courses :** دوره‌های متنوع SQL، طراحی پایگاه داده و مدیریت پایگاه داده‌های NoSQL .

۴- **SQL Server Management Studio (SSMS) :** آموزش کار با ابزار SQL Server Management Studioبرای مدیریت پایگاه داده‌ها.

۵- **Amazon RDS (Relational Database Service) :** دوره برای کار با پایگاه داده‌های رابطه‌ای در AWS .



با تشکر از همراهی شما

محمد سعید صفایی صادق