سوال 1: پروتکلهای HTTP و FTP هر دو برای انتقال داده در شبکه استفاده میشوند. تفاوتهای کلیدی این دو پروتکل را از نظر ساختار ارتباطی، پورتهای مورد استفاده و نحوه انتقال داده توضیح دهید.

جواب:

HTTP (پروتکل انتقال ابرمتن) از پورت ۸۰ استفاده می‌کند و معمولاً برای انتقال صفحات وب و داده‌های مبتنی بر وب به کار می‌رود. این پروتکل بدون حالت (Stateless) است، یعنی هر درخواست مستقل از درخواست‌های قبلی است.

از طرفی، **FTP** (پروتکل انتقال فایل) از پورت ۲۱ برای کنترل و پورت‌های دیگر برای انتقال داده استفاده می‌کند و برای انتقال فایل‌ها بین کلاینت و سرور طراحی شده است. FTP حالت‌دار (Stateful) است و نیاز به احراز هویت دارد، در حالی که HTTP معمولاً نیازی به احراز هویت ندارد. همچنین، FTP از دو کانال مجزا برای کنترل و انتقال داده استفاده می‌کند، در حالی که HTTP تنها از یک کانال برای هر دو منظور استفاده می‌کند.

سوال 2: سه مورد از معروفترین Web Server های رایج را نام ببرید و ویژگیهای کلیدی هر یک را توضیح دهید.

جواب:

1. **Apache HTTP Server:**
   - یکی از قدیمی‌ترین و پراستفاده‌ترین وب سرورهاست.
   - متن‌باز (Open Source) و قابل اجرا روی سیستم‌عامل‌های مختلف.
   - پشتیبانی از ماژول‌های گسترده برای افزودن قابلیت‌های مختلف.
   - انعطاف‌پذیری بالا و پشتیبانی از پروتکل‌های متعدد.
2. **Nginx:**
   - به دلیل عملکرد بالا و مصرف کم منابع معروف است.
   - مناسب برای سایت‌های پرترافیک و بارگذاری سنگین.
   - از پروکسی معکوس (Reverse Proxy) و بارگذاری متوازن (Load Balancing) پشتیبانی می‌کند.
   - سبک‌وزن و سریع، با پیکربندی ساده‌تر نسبت به Apache.
3. **Microsoft IIS:**
   - وب سرور مایکروسافت که مخصوص سیستم‌عامل ویندوز طراحی شده است.
   - ادغام خوب با دیگر محصولات مایکروسافت مانند ASP.NET
   - پشتیبانی از پروتکل‌های پیشرفته و امنیتی.
   - مناسب برای محیط‌های سازمانی که از فناوری‌های مایکروسافت استفاده می‌کنند.

سوال 3: چگونه میتوان امنیت یک سرور FTP را افزایش داد؟ دو روش مهم برای ایمن سازی ارتباطات FTP را نام ببرید و توضیح دهید.

جواب:

دو روش مهم برای ایمن‌سازی ارتباطات FTP عبارتند از:

1. **استفاده از FTPS (FTP Secure)** :
   - FTPS نسخه امن‌شده FTP است که از پروتکل‌های SSL/TLS برای رمزنگاری داده‌ها استفاده می‌کند.
   - این روش ارتباطات بین کلاینت و سرور را رمزنگاری می‌کند و از دسترسی غیرمجاز و استراق سمع جلوگیری می‌کند.
   - FTPS از دو حالت **Implicit** (پورت 990) و **Explicit** (پورت 21) پشتیبانی می‌کند.
2. **استفاده از SFTP (SSH File Transfer Protocol)** :
   - SFTP برخلاف FTPS، از پروتکل SSH برای انتقال فایل‌ها استفاده می‌کند.
   - این روش تمام ارتباطات، از جمله احراز هویت و انتقال داده‌ها، را از طریق SSH رمزنگاری می‌کند.
   - SFTP معمولاً از پورت 22 استفاده می‌کند و به دلیل امنیت بالا و سادگی در پیکربندی، گزینه مناسبی برای انتقال امن فایل‌ها است.

هر دو روش FTPS و SFTP امنیت ارتباطات FTP را به‌طور قابل توجهی افزایش می‌دهند و باعث جلوگیری از حملات رایج مانند sniffing و brute force میشوند.

سوال 4: در سرورهای HTTP، مفهوم "Virtual Host" چیست و چگونه میتوان از آن برای میزبانی چندین وبسایت روی یک سرور استفاده کرد؟

جواب:

Virtual Host (میزبان مجازی) در وب سرورهایی مانند Apache وNginx ، قابلیتی است که به شما امکان می‌دهد چندین وب‌سایت را روی یک سرور فیزیکی میزبانی کنید. این کار با استفاده از یک IP واحد یا چند IP انجام می‌شود. دو روش اصلی برای پیاده‌سازی Virtual Host وجود دارد:

1. **Name-based Virtual Host:**
   - در این روش، چندین دامنه (Domain) به یک IP آدرس متصل می‌شوند.
   - وب سرور با بررسی هدر **Host** در درخواست HTTP، تشخیص می‌دهد که کاربر به کدام وب‌سایت درخواست داده است.
   - مثال: اگر دو دامنه example.com و test.com به یک IP اشاره کنند، وب سرور بر اساس هدر Host، محتوای مناسب را به کاربر نمایش می‌دهد.
   - این روش مقرون‌به‌صرفه است، زیرا تنها به یک IP نیاز دارد.

2. **IP-based Virtual Host:**

- در این روش، هر وب‌سایت به یک IP اختصاصی متصل می‌شود.
- وب سرور بر اساس IP درخواست‌دهنده، وب‌سایت مناسب را ارائه می‌دهد.
- این روش زمانی استفاده می‌شود که نیاز به پشتیبانی از پروتکل‌های قدیمی‌تر مانند (SSL/TLS) باشد که از هدر Host پشتیبانی نمی‌کنند.