سوال1 :

الف) در مورد دو مدل هفت لایه OSI و TCP/IP توضیحاتی ارایه دهید.

- **مدل OSI**

این مدل دارای ۷ لایه است که این لایه‌ها عبارتند از:

1. **لایه فیزیکی (physical layer):** انتقال داده‌ها از طریق کابل، امواج رادیویی و...
2. **لایه پیوند داده (Data Link):** کنترل خطا و آدرس‌دهی فیزیکی
3. **لایه شبکه (Network):** مسیریابی و ارسال بسته‌ها بین دستگاه‌های مختلف.
4. **لایه انتقال (Transport):** ارائه انتقال مطمئن داده توسط پروتکل‌هایی مثل TCP وUDP
5. **لایه نشست (Session):** مدیریت نشست‌ها و ارتباطات بین دستگاه‌ها.
6. **لایه ارائه (Presentation):** رمزگذاری، فشرده‌سازی و ترجمه داده‌ها.
7. **لایه کاربرد (Application):** واسط کاربر با شبکه مانند HTTP ، FTP

- **مدل TCP/IP**

مدل TCP/IP کاربردی‌تر و رایج‌تر از OSI است و دارای ۴ لایه به‌شرح زیر است:

1. **لایه واسط شبکه (Network interface):** ترکیبی از لایه‌های فیزیکی و پیوند داده درOSI
2. **لایه اینترنت (Internet):** مشابه لایه شبکه درOSI ، شامل پروتکل‌هایی مانند IP وICMP
3. **لایه انتقال (Transport):** مشابه لایه انتقال در OSI وشامل پروتکل‌های TCP و UDP برای ارسال داده‌ها
4. **لایه کاربرد (Application):** ترکیب سه لایه بالایی مدل OSI ، شامل پروتکل‌هایی مانندHTTP ، FTP وSMTP

ب) عملکرد لایه شبکه هر دو مدل را بررسی کنید (چه عملیاتی انجام میشود. تفاوت این لایه در دو مدل و ...)

عملکرد کلی لایه شبکه در هر دو مدل شامل فعالیت های (مسیریابی داده از مبدا به مقصد، مدیریت آدرس‌دهی، هدایت بسته‌ها از طریق مسیریاب‌ها، شناسایی و رفع مشکلات مسیریابی مانند قطعی لینک ها) میشود.

تفاوت‌ها:

- در مدل **OSI**، لایه شبکه تنها بر مسیریابی تمرکز دارد، اما در مدل **TCP/IP**، این لایه با عنوان **لایه اینترنت** نیز شناخته می‌شود و شامل پروتکل‌هایی مانند IP، ICMP و ARP است.
- مدل TCP/IP به‌صورت عملیاتی‌تر توسعه یافته است، در حالی که OSI بیشتر به‌عنوان یک مدل نظری مطرح است.

سوال2 :

الف) اصطلاح sniffer به چه معناست؟

Sniffer به ابزاری گفته می‌شود که برای نظارت و ضبط بسته‌های داده‌ای که در یک شبکه منتقل می‌شوند، استفاده می‌شود. معمولا برای اهدافی مانند عیب‌یابی شبکه ویا شنود اطلاعات استفاده میگردد.

ب) دو بخش مهم عملکردی آن را (packet analyzer, packet capture library) را توضیح دهید.

کتابخانه ضبط بسته‌ها (Packet Capture Library) :

این بخش مسئول دریافت بسته‌های داده از کارت شبکه است. ابزارهای معروف مانند **libpcap** (در لینوکس) و **WinPcap** (در ویندوز) از این نوع کتابخانه‌ها استفاده می‌کنند.

تحلیل‌گر بسته‌ها (Packet Analyzer) :

این بخش داده‌های خام را پردازش و تجزیه وتحلیل می‌کند و اطلاعاتی مانند آدرس‌هایIP ، پورت‌ها، نوع پروتکل و محتوای بسته‌ها را نمایش می‌دهد. ابزارهایی مانند **Wireshark** و **tcpdump** برای تحلیل بسته‌های شبکه استفاده می‌شوند.

سوال3 : در مورد نرم افزار wireshark و کاربردهای آن در تحلیل ترافیک شبکه توضیحاتی ارایه دهید.

Wireshark یک نرم‌افزار متن‌باز و رایگان برای **آنالیز و بررسی ترافیک شبکه** است. این ابزار به کاربران اجازه می‌دهد تا بسته‌های داده‌ای که در یک شبکه در حال تبادل هستند را **ضبط، مشاهده و تحلیل** کنند.

کاربردهای Wireshark :

عیب‌یابی شبکه(Network Troubleshooting) : تشخیص مشکلاتی مانند تأخیر، بسته‌های ازدست‌رفته، تداخل شبکه و پیکربندی‌های اشتباه

تحلیل امنیت شبکه(Network Security Analysis) : شناسایی حملاتی مانند Man-in-the-Middle (MITM)، Sniffing و DoS Attack و بررسی تلاش‌های مشکوک برای دسترسی غیرمجاز به سیستم‌ها

مانیتورینگ عملکرد شبکه(Network Performance Monitoring) : اندازه‌گیری میزان استفاده از پهنای باند

آموزش و یادگیری شبکه(Educational Purposes) : تحلیل رفتار پروتکل‌ها برای درک بهتر ساختار شبکه و بسته‌های داده و بررسی نحوه ارسال و دریافت داده‌ها در لایه‌های مختلف مدل OSI و TCP/IP

تحلیل پروتکل‌ها و توسعه نرم‌افزارهای شبکه: بررسی نحوه کارکرد پروتکل‌های سفارشی و تشخیص مشکلات احتمالی و تست عملکرد API های شبکه و سرویس‌های اینترنتی.