۱. هر یک موارد زیر را با ذکر یک مثال توضیح دهید.

Authentication
Authorization
Availability
Software Modification
Integrity

۲. چه رابطه ای بین آسیب پذیری و تهدید وجود دارد؟ توضیح دهید.
۳. تفاوت بین تهدیدات امنیتی passive و active چیست؟
۴. انواع تهدیدات را نام برده و توضیح دهید.
۵. آیا اتصال TCP در برابر استراق سمع ایمن است؟ چرا؟
۶. نمونه هایی از replay attacks را ذکر کنید.
۷. در صورت به خطر افتادن یکپارچگی یک برنامه یا داده های شرکت، سه نوع آسیب را که یک شرکت متحمل می‌شود، نام ببرید
۸. SSL چیست و از چه نوع رمزنگاری استفاده میکند؟ توضیح دهید.
۹. SSL برای رسیدن به چه هدفی از MAC استفاده میکند؟
۱۰. برای جلوگیری از حملات sniffing در ترافیک برنامههای تحت وب، استفاده از چه پروتکلی را پیشنهاد می‌دهید؟ چرا؟
۱۱. تفاوت بین امضای دیجیتال direct و arbitrated چیست؟
۱۲. VPN از رمزگذاری متقارن استفاده می کند یا نامتقارن ؟ پاسخ خود را توضیح دهید.