درس امنیت شبکه

تمرین– معماری امنیت شبکه

س ۱– حمله های شبکه را از چند دید دسته بندی می کنند. در جدول زیر سه نوع دسته بندی آمده است:

Classification 1	Classification 2	Classification 3
Interruption Interception Modification Fabrication	Denial of Service Reconnaissance Illegal Access	Denial of Service Masquerade Passive monitoring Replay Modification of message content

الف– نمونه ای از هر یک از این حملات را ذکر کنید.

ب– نگاشتی بین این دسته بندیها انجام دهید و پاسخ خود را توجیه کنید.

س ۲– با مطالعه استاندارد X.800 به موارد زیر پاسخ دهید:

الف– انواع سرویسها و مکانیسمهای امنیتی مطرح برای هر یک از لایه های OSI را بنویسید.

ب– ابعاد مدیریت امنیت را بنویسید.

س ۴– از RFC4778 لیستی از روشهای امنیتی جاری در شبکه‌های Service Provider ها را تهیه کنید.

س ۵– از RFC3682 روش GTSM را تشریح کنید.

سئوالات زیر را از کتاب NSE پاسخ دهید.

سئوال ۶:

For each of the following assets, assign a low, moderate, or high impact level for the loss of confidentiality, availability, and integrity, respectively. Justify your answers.

a. An organization managing public information on its Web server.

b. A law-enforcement organization managing extremely sensitive investigative information.

c. A financial organization managing routine administrative information (not privacy-related information).

d. A power plant contains a SCADA (supervisory control and data acquisition) system controlling the distribution of electric power for a large military installation. The SCADA system contains both real-time sensor data and routine administrative information. Assess the impact for the two data sets separately and the information system as a whole.

سئوال ۷:

Draw a matrix similar to Table 1.4 (based on X.800) that shows the relationship between security services and attacks.

سئوال ۸:

Draw a matrix similar to Table 1.4 (based on X.800) that shows the relationship between security mechanisms and attacks.