*** مرجع : فصل ۱ نسخه ۵ کتاب Network Security Essentials

۱. (سوال ۱.۴ از کتاب) توضیح دهید چرا شناسایی حملات passive و جلوگیری حملات active دشوار است ؟

۲. (سوال ۱.۱ از کتاب) یک دستگاه ATM را در نظر بگیرید که با کمک کارت و یک پین اجازه دسترسی به اطلاعات را برای کاربران فراهم میکند . نیازمندی های این سیستم را برای تامین confidentiality ، integrity و availability بیان کنید و در هر مورد میزان اهمیت نیازمندی را با low، moderate و high مشخص کنید .

۳. (سوال ۱.۳ از کتاب) یک سیستم تولید مستندات را در نظر بگیرید که برای تولید مستندات در زمینه های مختلف در سازمانهای گوناگون به کار گرفته میشود . برای هر یک از موارد زیر برای این سیستم یک کاربرد مثال بیاورید :

- سیستمی که محرمانگی اطلاعات ذخیره شده از دو معیار دیگر مهم تر باشد .
- سیستمی که صحت داده از سایر معیارهای امنیت اهمیت بیشتری داشته باشد .
- سیستمی که در آن در دسترس بودن مهم ترین معیار امنیتی باشد .

۴. برای هرکدام از انواع حملات زیر یک نمونه از دنیای واقعی بیاورید و یک مکانیزم امنیتی برای آن پیشنهاد دهید .

- حمله replay
- حمله DOS
- حمله IP Spoofing

۵. با مراجعه به سایت https://www.cvedetails.com سه نمونه از آسیب پذیری های گزارش شده را بیابید و به طور مختصر توضیح دهید که هرکدام از این آسیب پذیری ها چگونه باعث ایجاد یک تهدید امنیتی برای سیستم شده اند .

۶. در هر یک از موارد زیر مشخص کنید که حمله از چه نوعی بوده است و به طور کوتاه توضیح دهید که برای چه معیارهایی از امنیت اختلال ایجاد شده است .

- در تاریخ ۲۰ سپتامبر ۲۰۱۶ ، مهاجم با به کارگیری شبکهای از botNet ها به صورت توزیع شده و اشغال کردن ترافیک زیاد شبکه باعث شد که کاربران مرکز داده ی OVH تا حدی در گرفتن سرویس از این مرکز داده دچار مشکل شوند .
- مهاجم با ساختن یک صفحه درست مشابه صفحه سایت ورود و قرار دادن لینک آن در یک ایمیل ارسالی برای کاربران توانسته است اطلاعات حساب تعداد زیادی از کاربران را به دست آورد .
- در سال ۲۰۱۴ یک مهاجم با به کارگیری آسیب پذیری موجود در سیستم OPM در آمریکا به اطلاعات ۲۲ میلیون از کاربران این سیستم دست یافت .

۷. سه نمونه از ابزارهای موجود برای فراهم کردن مکانیزم های امنیتی در سیستم ها را بیابید و مشخص کنید هر کدام چه مکانیزم هایی جهت تامین امنیت در اختیار کاربران قرار میدهند .

- پاسخ تمرینات حدالامکان به صورت **تایپ شده و فایل PDF** تحویل داده شود. در صورت عدم امکان تایپ پاسخ تمرین ، عکسی واضح از برگه پاسخ تهیه و به فرمت PDF در آورید. (برای اینکار میتوانید از camScanner و امثال آن استفاده کنید.)
- فرمت نامگذاری پاسخ به صورت **HW1_StdNO_StdName** باشد.
- پاسخ تمرینات حتما قبل از موعد تحویل در مودل بارگذاری شوند. تمریناتی که بعد از موعد تحویل ارسال شوند ، **تصحیح نخواهد شد.**
- در صورت مشاهده **تقلب** برای طرفین **نمره صفر** در نظر گرفته می شود.
- در صورت وجود هر گونه سوال یا اشکال در رابطه با تمرین از آدرس ایمیل f.dehghan@aut.ac.ir استفاده کنید.