شروع	سه‌شنبه، 3 خرداد 1401، 4:05 عصر
وضعیت	پایان‌یافته
پایان	سه‌شنبه، 3 خرداد 1401، 4:19 عصر
زمان صرف شده	14 دقیقه 1 ثانیه
جمع نمره	9.00 از 11.00
نمره	**8.18** از 10.00 (**82**٪)

سؤال 1

پاسخ نیمه درست

نمره 0.50 از 2.50

کدام یک از گزینه های زیر از کاربردهای IPsec نمیباشد؟

یک یا چند گزینه را انتخاب کنید:

- a. تضمین تازگی
- b. پروتکل تبادل کلید ✗
- c. رمزگذاری بسته ها
- d. تامین یکپارچگی در ارتباط همراه با اتصال ✓
- e. پروتکل توافق کلید
- f. فرایند احراز اصالت

پاسخ شما تا حدودی صحیح است

شما به درستی 1 گزینه را انتخاب کرده‌اید

پاسخ درست عبارت است از:

تامین یکپارچگی در ارتباط همراه با اتصال,

پروتکل توافق کلید

سؤال 2

درست

نمره 2.00 از 2.00

گزینه مناسب را برای هر یک از موارد زیر انتخاب کنید:

در این روش محتوای سربسته لایه انتقال مورد بازرسی قرار میگیرد.	طبقه بندی ترافیک بر مبنای محتوا ✔
تنها یکپارچگی که به منظور احراز اصالت، یکپارچگی و جلوگیری از حمله بازپخش استفاده میشود.	AH ✔
یک سمت کلید را تولید کرده و در اختیار طرف مقابل قرار میدهد.	Key Transport ✔
ویژگی های آماری سربسته و محتوای بسته انتقال مورد پویش قرار میگیرد.	SPI ✔

پاسخ شما صحیح می باشد

پاسخ درست:
در این روش محتوای سربسته لایه انتقال مورد بازرسی قرار میگیرد. → طبقه بندی ترافیک بر مبنای محتوا,
تنها یکپارچگی که به منظور احراز اصالت، یکپارچگی و جلوگیری از حمله بازپخش استفاده میشود. → AH,
یک سمت کلید را تولید کرده و در اختیار طرف مقابل قرار میدهد. → Key Transport,
ویژگی های آماری سربسته و محتوای بسته انتقال مورد پویش قرار میگیرد. → SPI

سؤال 3

درست

نمره 2.00 از 2.00

کدام گزینه غلط است و کدام صحیح؟

در PKI صحبتی از بحث‌های سخت‌افزاری در حوزه مدیریت کلید صورت نمی‌پذیرد.	غلط ✔
تنها راه برای اطمینان بخشی از صحت تبادل کلید عمومی، استفاده از یک مرجع متمرکز به عنوان مرجع ثالث مورد اعتماد است.	غلط ✔
در زنجیره گواهینامه، Root CA تنها CA است که می‌تواند گواهینامه خودش را امضا کند (*self-signed*)	صحیح ✔
روند امضای یک گواهینامه بدین صورت است که کل متن گواهینامه با کلید خصوصی CA رمز می‌شود و در اختیار فرد قرار می‌گیرد.	غلط ✔

پاسخ شما صحیح می باشد

پاسخ درست:

در PKI صحبتی از بحث‌های سخت‌افزاری در حوزه مدیریت کلید صورت نمی‌پذیرد. → غلط,

تنها راه برای اطمینان بخشی از صحت تبادل کلید عمومی، استفاده از یک مرجع متمرکز به عنوان مرجع ثالث مورد اعتماد است. → غلط, در زنجیره گواهینامه، Root CA تنها CA است که می‌تواند گواهینامه خودش را امضا کند (*self-signed*) → صحیح,

روند امضای یک گواهینامه بدین صورت است که کل متن گواهینامه با کلید خصوصی CA رمز می‌شود و در اختیار فرد قرار می‌گیرد. → غلط

سؤال 4

درست

نمره 2.50 از 2.50

صحیح یا غلط بودن هر یک از گزاره های زیر را مشخص کنید:

امنیت میتواند در لایه کاربرد یا بین لایه انتقال و لایه شبکه باشد.	غلط ✔
TLS در حالت کلی پیچیده تر از IPsec است.	غلط ✔
در TLS کاربرد باید تغییر کند ولی در IPsec سیستم عامل باید تغییر کند.	صحیح ✔
IPsec مجموعه ای از پروتکل هاست که میتواند امنیت را در لایه کاربرد به وجود آورد.	غلط ✔
در Transport Mode فقط محتوا لایه شبکه رمز میشود.	صحیح ✔

پاسخ شما صحیح می باشد

پاسخ درست:
امنیت میتواند در لایه کاربرد یا بین لایه انتقال و لایه شبکه باشد. → غلط,
TLS در حالت کلی پیچیده تر از IPsec است. → غلط,
در TLS کاربرد باید تغییر کند ولی در IPsec سیستم عامل باید تغییر کند. → صحیح,
IPsec مجموعه ای از پروتکل هاست که میتواند امنیت را در لایه کاربرد به وجود آورد. → غلط,
در Transport Mode فقط محتوا لایه شبکه رمز میشود. → صحیح

سؤال 5

درست

نمره 1.50 از 1.50

کدام‌یک از موارد زیر از پارامترهای فیلد گواهی نامه نیست؟

یک یا چند گزینه را انتخاب کنید:

- [ ] **امضا**
- [ ] **شناسه یکتای سوژه**
- [ ] **نام صادر کننده**
- [x] **اصلاح کننده سریال**
- [ ] **نام سوژه**

پاسخ شما صحیح می باشد

پاسخ درست « **اصلاح کننده سریال** » است.

سؤال 6

درست

نمره 0.50 از 0.50

روند امضای یک گواهینامه بدین صورت است که کل متن گواهینامه با کلید خصوصی CA رمز می‌شود و در اختیار فرد قرار می‌گیرد.

- غلط
- صحیح

پاسخ شما صحیح می باشد

پاسخ درست « غلط» است.