دانشگاه صنعتی امیرکبیر
دانشکده مهندسی کامپیوتر

دکتر حمیدرضا شهریاری

مهدی نیکوقدم

پاییز۱۴۰۱

۱. سه روش که می‌تواند امنیت اعتبارسنجی کاربر در یک محیط توزیع شده را بهبود دهد بیان کنید؟

۲. چهار نیازی که برای Kerberos تعریف شده است کدامند؟

۳. تفاوت‌های بین ورژن ۴ و ۵ Kerberos در چیست؟

۴. هدف از استفاده کلید جلسه در Kerberos چیست؟

۵.تفاوت بین توافق کلید و تبادل کلید در چیست؟ کدام سربار کمتری دارند؟ در چه زمانی از توافق کلید و در چه زمانی از تبادل کلید استفاده می‌کنیم؟

۶. تفاوت مفاهیم Connection و Session در SSL را بیان کنید.

۷. عناصر کلیدی در گواهی X.509 را نام ببرید.

۸. درSSL و TLS چرا به جای اینکه تنها یک پیام change_cipher_spec در پروتکل Handshake وجود داشته باشد، یک پروتکل Change Cipher Spec جداگانه فراهم شده است.

۹. تهدیدهای زیر در مورد امنیت web در نظر بگیرد و عنوان کنید که چگونه با هر یک از آن‌ها توسط یکی از مشخصه‌های SSL مقابله می‌شود.

الف.IP Spoofing:با استفاده از آدرس‌های IP جعلی یک میزبان را گول زده تا دیتای جعلی را بپذیرد.

ب. password sniffing: کلمات عبور در HTTP و یا سایر کاربردها مورد استراق سمع قرار میگیرد.

ج. حمله بازخوانی : پیام‌های handshake قدیمی دوباره اجرا شوند.

۱۰.پارامترهایی که حالت Session را تعریف می‌کنند را بیان کرده و مختصرا توضیح دهید.

۱۱. تعریف شما از مرکز توزیع کلید چیست و راه‌های ممکن برای توزیع یک کلید سری بین دو واحد را نام ببرید.

۱۲. منظور از ISAKMP یا (Internet Security Association and Key Management Protocol) چیست؟

۱۳. نقش پروتکل ISAKMP در IPSec چیست؟

۱۴. به لینک https://sslcheck.cert.ir/fa/ و یا https://sslcheck.certcc.ir مراجعه کنید و بعد از مطالعه و فهم مسئله‌ای که هدف سایت است، ۳ سایت را به دلخواه از نظر امنیتی بررسی کنید و نتایج را به صورت اسکرین در PDF قرار دهید.

- **عکسی واضح از برگه پاسخ تهیه و به فرمت pdf در آورید و آپلود کنید.**
- **فرمت نامگذاری پاسخ به صورت HW4_StdNO_StdName باشد.**
- **پاسخ تمرینات حتما قبل از موعد تحویل اعلام شده در هر سری، بارگذاری شوند. تمریناتی که بعد از موعد تحویل ارسال شوند به هیچ عنوان تصحیح نخواهند شد.**
- **در صورت مشاهده تمرینات کپی شده برای طرفین نمره صفر در نظر گرفته می‌شود.**

هدف افزایش یادگیری است!

مهدی نیکوقدم