مبانی رایانش امن

تمرین چهارم

فایل‌های پاسخ خود را با الگوی HW4-9431XXX-StudentName.pdf نامگذاری نمایید.
در صورت مشاهده تقلب برای طرفین نمره صفر درنظر گرفته خواهد شد.
در صورت وجود هرگونه اشکال یا سوالی از طریق ایمیل alireza97hi@gmail.com موارد را بیان کنید.

تمرینات فصل‌های SSL, IPSEC , EMAIL SECURITY

۱. برای هر یک از ابعاد امنیت (integrity, confidentiality, denial of service, authentication) موارد تهدید، عواقب (threats, consequences) در جهان وب را بیان کنید.

۲.دو ایده و مفهوم اساسی در پی‌ریزی SSL یعنی connection و session را تعریف کنید.

۳.پروتکل‌های SSL را نام برده و مشخص کنید در هر یک از حالت‌های زیر از کدام پروتکل‌های SSL میتوان استفاده کرد:

الف)شناسایی کارفرما و کارگزار قبل از مبادله اطلاعات

ب) فشرده‌سازی و رمزنگاری داده‌ها

ج)محاسبه MAC

۴.مشخص کنید هر یک از موارد زیر در کدام دسته از انواع کانال‌های SSHقرار می‌گیرند:

الف) با کمک کتابخانه libssl یک ترمینال مجازی به یک ماشین مجازی در سیستم با آدرس مشخص ایجاد می‌کنید و دستورات لازم را در این ترمینال در ماشین مجازی به اجرا در می‌آورید.

ب) با ارتباط گرافیکی به یک سرور از طریق SSH امکان تبادل اطلاعات با سرور و دریافت نتیجه به صورت گرافیکی پس از پردازش در سرور روی سیستم درخواست کننده فراهم می‌شود.

ج) یک کلاینت 3POP روی سیستم داریم که به کمک SSH یک پورت جدید روی سیستم را برای تبادل امن تعیین می‌کنیم و این پورت جدید را برای تبادل به اطلاع سرور می‌رسانیم.

۵.موارد استفاده از Transport Mode و Tunnel Mode در دو حالت AH و ESP را بیان کنید.

۶.طول و و موارد استفاده‌ی هریک از فیلدهای زیر در Authentication Header را بیان کنید.
الف) Next Header

ب) Payload Length

ج) Reserved

د) Sequence Number

۷. روش‌های مدیریت دو زوج کلید AH و ESP جهت انتقال و دریافت را بیان کنید.

۸. چه محدودیت‌هایی باعث شد تا PGP جایگزین قراردادهای SMTP و MIME شود؟ الگوریتم‌های رمزنگاری استفاده شده در PGP را نام ببرید.

۹.نقش و مراحل روند ایجاد حفظ سازگاری در پروتکل PGP را بیان کنید و چگونگی فشرده‌سازی پیام‌ها به کمک الگوریتم‌ها و میزان فشرده‌سازی را مشخص کنید.