به نام خدا

تمرین چهارم امنیت داده و شبکه

نیم‌سال دوم ۱۴۰۳-۱۴۰۲

دانشکده مهندسی کامپیوتر

دانشگاه صنعتی شریف

موضوع **امنیت شبکه**

موعد تحویل **ساعت ۲۳:۵۹ یکشنبه ۱۳ خرداد ۱۴۰۳**

طراحی تمرین توسط **رضا سعیدی**

۱ Pretty Good Problem

در این سؤال از پروتکل PGP برای اجرای یک سناریو ساده استفاده خواهیم کرد.

- می‌توانید از ابزار GnuPG و یا کتابخانه پایتون PGPy استفاده نمایید.
- قسمت‌هایی که با * نشان داده شده است بیانگر الزام ارائه تصویر از مراحل انجام کار است.

با توجه به نکات فوق به سؤالات زیر پاسخ دهید:

(آ) یک جفت کلید عمومی و خصوصی PGP با نام و ایمیل خود بسازید. *

(ب) اطلاعات کلیدهای خود را مشاهده کرده [۱] و شناسه کلید عمومی، الگوریتم‌های استفاده شده برای رمزگذاری، امضا و چکیده را مشخص کنید. *

(پ) کلید عمومی خود را در سرور کلید keys.openpgp.org ثبت کرده و آدرس ایمیل خود را نیز تائید کنید. سپس از مبدأ همان آدرس،یک ایمیل با عنوان PGP-STDID منظور از STDID شماره دانشجویی شماست) و محتوای نام و شماره دانشجویی خود به آدرس pgpot@mailo.com ارسال کنید. پیام ارسالی باید امضاشده و همچنین رمزشده با کلید عمومی گیرنده باشد. سپس پاسخ ایمیل دریافتی را با کلید خصوصی خود رمزگشایی کرده و محتوای آشکار آن را عیناً به عنوان پاسخ سؤال بیاورید [۲].

(ت) اگر شخصی ایمیل امضا شده شما را دریافت کند، آیا واقعاً اطمینان دارد که این ایمیل از طرف شما آمده است؟ توضیح دهید.

(ث) آیا شما به عنوان ارسال کننده پیام مطمئن هستید که فقط دریافت کننده پیام می تواند ایمیل شما را بخواند؟ توضیح دهید.

(ج) در این سؤال برای ثبت و انتقال کلید عمومی از یک سرور کلید عمومی استفاده شد. با در نظر گرفتن روش احراز مالکیت ایمیل در این سرور کلید بررسی کنید آیا امکان دارد مهاجمی با داشتن دسترسی به سرور ایمیل حمله مرد میانی را اجرا کند؟

۲ SSL/TLS

مسئولیت ارزیابی امنیت یک برنامه وب که از SSL/TLS برای ارتباط استفاده می‌کند به شما سپرده شده است.

(آ) نقش SSL/TLS در امن‌کردن ارتباطات وب را توضیح دهید و ویژگی‌ها و مکانیزم‌های کلیدی آن را توضیح دهید.

(ب) توضیح دهید چگونه یک مهاجم می‌تواند از ضعف‌های SSL/TLS بهره‌برداری کند و امنیت یک برنامه وب را تهدید کند.

(پ) SSLLab یک ابزار برخط برای تجزیه و تحلیل پیکربندی SSL/TLS یک سرور وب است. چرا تایید گواهی نامه یک وبسایت اهمیت دارد؟ توضیح دهید که SSLLab چگونه می‌تواند برای این منظور استفاده شود. سایت اصلی دانشگاه و سامانه aibuz را با استفاده از این ابزار اسکن کنید و و نتایج آن را توضیح دهید (تصاویر و مراحل انجام کار در گزارش آورده شود).

(ت) BurpSuite یک پلتفرم جاوا محور برای تست امنیت برنامه‌های تحت وب است. یک سامانه به دلخواه انتخاب کنید و با استفاده از این ابزار ترافیک SSL/TLS بین مرورگر خود و سرور را ضبط کنید. آیا امکان تغییر بسته های ارسالی به سرور از طریق این ابزار وجود دارد؟ توضیح دهید. (تصاویر و مراحل انجام کار در گزارش آورده شود)

---

[۱] می‌توانید از ابزار pgpdump استفاده نمایید.

[۲] می‌توانید برای انجام عملیات رمزگذاری و امضا از واسط وب رایانامه دانشگاه استفاده کنید. راهنمای استفاده از این واسط این ارائه شده است.

۳ دیوار آتش

پروتکل SMTP برای انتقال ایمیل روی TCP است. در این پروتکل سرور بر روی درگاه[۳] ۲۵ به درخواست‌ها گوش می‌کند و کارخواه با درگاه مبدأ بالاتر از ۱۰۲۳ به آن متصل می شود. فرض کنید یک دیوار آتش در سطح بسته برای کنترل ارسال و دریافت ایمیل با چنین قواعدی طراحی شده است:

قاعده	جهت	آدرس مبدا	آدرس مقصد	پروتکل	درگاه مقصد	عملیات
آ	داخل	خارجی	داخلی	TCP	۲۵	مجاز
ب	خارج	داخلی	خارجی	TCP	>۱۰۲۳	مجاز
ج	خارج	داخلی	خارجی	TCP	۲۵	مجاز
د	داخل	خارجی	داخلی	TCP	>۱۰۲۳	مجاز
ه	هر دو	هر	هر	هر	هر	رد

(آ) هدف هر یک از قواعد فوق چیست؟ توضیح دهید.

(ب) یک نفر از بیرون با آدرس 10.1.2.3 و درگاه ۵۱۵۰ سعی میکند به پروکسی که داخل شبکه محلی با آدرس 172.16.3.4 و روی درگاه ۸۰۸۰ در حال سرویس دهی است، وصل شود .آیا این فرد امکان اتصال را می‌یابد؟

(پ) قواعد جدول بالا را با استفاده از iptables پیاده‌سازی کنید. برای این کار نیاز به دسترسی سطح root در توزیع دلخواه از سیستم عامل Linux دارید. می‌توانید از ماشین مجازی برای راه اندازی محیط مورد نیاز استفاده کنید. در هر مورد فیلمی از مراحل اجرا و صحت عملکرد ارائه کرده و پاسخ خود را توضیح دهید.

[3] Port