۱- C,S,KDC[1] اعضای دامنه[2] کربروس هستند. زمانی که C درخواست بلیط برای S کند. KDC یک کلید موقت $K_{c,s}$ را ایجاد می‌کند. باتوجه به این که KDC کلید $K_{c,s}$ را می‌داند، می‌تواند تمام ترافیکی که با این کلید رمز نگاری می‌شود را رمزگشایی کند.

الف) با فرض این که KDC نمی‌تواند ترافیک بین C و S را تغییر دهد. C و S چطور می‌توانند یک کلید مشترک به نام K' بین خود تبادل کنند به طوری که KDC نتواند آن را بدست آورد.

ب) اگر KDC امکان تغییر ترافیک بین C و S را داشته باشد چگونه می‌تواند راه حل ارئه شده شما در بخش اول را تهدید کند؟

ج) فرض کنید C,S به طور همزمان عضو دو دامنه کربروس باشند به طوری که :

- دامنه ۱ : KDC1 که کلید $K_{c,s,1}$ را ایجاد کرده است
- دامنه ۲: KDC2 که کلید $K_{c,s,2}$ را ایجاد کرده است

با فرض این که KDC1 و KDC2 امکان تبانی ندارند ولی می‌توانند ترافیک بین C و S را تغییر دهند. C و S چطور می‌توانند یک کلید مشترک به نام K' بین خود تبادل کنند به طوری که KDC1 و KDC2 نتوانند آن را بدست آورند.

۲- با توجه به پروتکلPGPبه سؤالات زیر پاسخ دهید:

- الف) یک کارخواه ایمیل PGP راه اندازی کرده و یک زوج کلید برای خود بسازید. روند انجام کار را توضیح دهید.

ب) یک ایمیل رمز شده و امضا شده از ایمیل شریف خود به آدرس ایمیل reza.saeedi9@yahoo.com ارسال کنید (کلید عمومی نظیر این ایمیل در پیوست تمرین موجود است) به نحوی که عنوان ایمیل، نام شما ومتن ایمیل، شماره دانشجویی شما باشد. در گزارش خود، روند انجام کار را توضیح داده و فایل کلید عمومی خود را پیوست کنید.

[1] Key Distribution Center
[2] Realm

۳-به سوالات زیر پاسخ دهید:

الف) برای هر بخش توضیح دهید کدام یک از ویژگی های IPSec باعث جلوگیری از حمله‌های زیر می‌شود. (درهر قسمت ابتدا حمله‌ی نام برده شد را توضیح داده و عملکرد آن را شرح دهید سپس با ذکر دلیل، چگونگی جلوگیری پروتکل IPSec، از هر یک از حملات را با ذکر مد کارکردی وهمچنین خصوصیت تاثیر گذار بررسی کنید.)

- حمله‌ی جست وجوی فراگیر (Brute force cryptanalytic attack)
- حمله مبتنی بر متن اصلی معلوم (Known plaintext dictionary)
- حمله‌ی تکرار (Replay attack)
- شنود رمز عبور (Password sniffing)
- جعل IP (IP spoofing)
- سرقت IP (IP hijacking)
- حمله‌ی SYN flooding

ب) با استفاده از ابزار strongsawn بین دو گره (می‌توانید از دو ماشین مجازی استفاده کنید) یک ارتباط IPsec برقرار کنید و تصاویری از مراحل و نتیجه را ارائه دهید.

۴- به یکی از سایت‌های دلخواهتان که از پروتکل HTTPs استفاده می‌کند رفته و ترافیک عبوری را با نرم‌افزار wireshark ضبط کنید. سپس فیلتر را برابر ssl قرار داده تا تنها فریم‌های دریافتی/ارسالی شامل رکوردهای ssl را نشان دهد. توجه کنید که یک فریم می‌تواند شامل چندین رکورد باشد هم چنین ممکن است یک رکورد برای ارسال نیاز به بیش از یک فریم داشته باشد.

الف) برای هشت تا فریم اول، مبدأ (این‌که سرور ارسال کرده یا کلاینت را مشخص کنید)، تعداد رکوردهای SSL و نام آنها را بنویسید و دیاگرامی از رکوردهای رد و بدل شده بین کلاینت و سرور را ترسیم کنید. همچنین هر رکورد شامل سه تا فیلد می‌شود، این فیلدها و طول آن‌ها چقدر است؟

ب) رکورد client Hello (اگر چندین فریم بود، اولی را بررسی کنید): Content type چیست؟ nonce یا همان challenge برابر چیست و چه استفاده‌ای از آن می‌شود؟ cybersuite های مختلفی که اعلان می‌کند و الگوریتم‌های متقارن و نامتقارن و تابع چکیده‌ساز چیست؟

پ) رکورد ServerHello: ciphersuite انتخابی و الگوریتم‌های آن چیست؟ آیا شامل nonce می‌شود؟ session ID چیست و از آن چه استفاده‌ای می‌شود؟ آیا شامل certificate می‌شود یا در یک فریم دیگر ارسال شده است؟ الگوریتم رمزنگاری کلید عمومی و طول کلید عمومی، الگوریتم امضا و مقدار امضا، صادرکننده گواهی (certificate issuer) آن چیست؟

ت) رکورد Client Key Exchange: مقدار pre-master secret برابر چیست و به چه منظور استفاده می‌شود؟

ث) رکورد Change Cipher Spec و Encrypted Handshake: این رکورد به چه مورد استفاده می‌شود؟ آیا مقداری که سرور می‌فرستد با کلاینت فرق دارد؟ چرا؟

ج) رکورد Application data: داده مورد نظر چگونه رمزنگاری می‌شود؟

۵- برای دیوار آتش iptables خط قوانینی بنویسید که کارهای زیر را انجام دهد:

(راهنمایی: https://www.netfilter.org/documentation/index.html#documentation-howto)

الف) اجازه دادن به عبور همه ترافیک‌های خروجی

ب) جلوگیری از ترافیک‌های ورودی به غیر از ارتباطاتی که established شده‌اند و همچنین ترافیک‌های ssh ورودی (خط قانون را بر روی پروتکل transport و پورت بنویسید)

پ) اجازه عبور و دریافت تمام ترافیک‌های ICMP به غیر از ICMP Redirect ها

ت) همه ترافیک ورودی به پورت ۸۰ را به پورت ۸۰۸۰ فوروارد کند.

ث) به جلوگیری از حملات منع سرویس در یک وب سرور کمک کند.

نکات مهم

- **خروجی تمرین شما می‌بایست دقیقا مطابق با استاندارد عنوان شده در زیر باشد.**

DNS-HW4-STDID.zip..... (STDID شماره دانشجویی شماست)
DNS-HW4-STDID.pdf

- اطمینان حاصل کنید که سند آشنایی با مقررات تمرینها را به خوبی مطالعه کرده و نسبت به نکات و دلایل احتمالی کسر نمره ذکر شده در آن آگاهی کامل را بدست آورده اید.
- در صورت استفاده از هر گونه منبع برای پاسخ به سوالات، ذکر اسم و نشانی دقیق و کامل دسترسی به صفحه مورد نظر الزامی است.