تمرین شماره ۴

درس: مبانی امنیت شبکه‌های کامپیوتری

نیمسال دوم سال تحصیلی ۰۵-۱۴۰۴

سوال ۱)

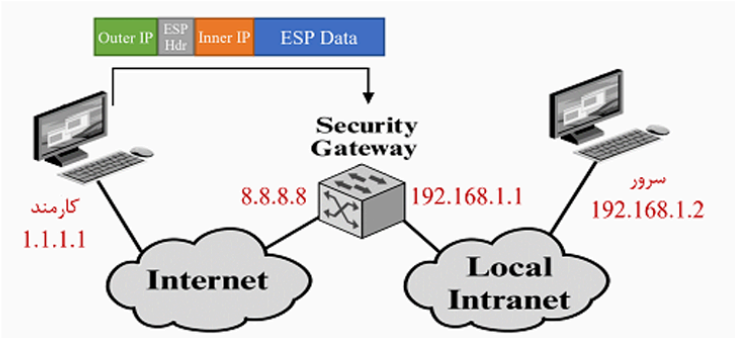
در شکل زیر یک کارمند برای دورکاری میخواهد با حالت تونل ESP به سرور داخلی شرکت وصل شود. او یک SA با gateway یا درگاه شرکت دارد. آدرس هر لینک برای هر میزبان در شکل نوشته شده است.

الف) چرا SA بین کارمند و سرور (به صورت H2H) ایجاد نشده است؟ به طور کلی بیان کنید چرا حالت تونل بین دو میزبان انتهایی ایجاد نمیشود.

ب) اگر کارمند بخواهد از AH هم استفاده کند، چرا توصیه شده است ابتدا ESP و سپس AH اعمال شود؟

ج) آیا لازم است IPSec سمت سرور هم پیاده سازی شود؟

د) آدرس مبداء و مقصد را در header یا سرآیند IP درونی و سرآیند IP بیرونی برای بسته ی مشخص شده در شکل بیان کنید کدام یک از آنها رمز شده اند؟



سوال ۲)

دو کاربر که هر دو پشت NAT هستند می خواهند با حالت انتقال ESP با یکدیگر ارتباط داشته باشند. این کار چگونه ممکن است به طوری که مشکل Checksum و (Port Address Translation) PAT پیش نیاید؟ (**راهنمایی:** در مورد IPSec NAT Traversal مطالعه کنید.)

سوال ۳)

سه فایل ترافیک ضبط شده (cap) برای نشست های از نوع SSL3 (+ کلید خصوصی RSA سرور) ، TLSv1.2 و TLSv1.3 (+ مقادیر محرمانه) ارائه شده است. با ابزار Wireshark آنها را باز کنید و به سؤالات هر قسمت با پیوست کردن اسکرین شات های کافی و مناسب پاسخ دهید.

در لینک زیر میتوانید، این سه فایل را داشته باشید:
https://drive.google.com/file/d/1zG_errx7nEvZiAD80Etu-Fcc1J4uQ1EK/view?usp=drive_link

در مورد ترافیک ضبط شده مربوط به SSL3 به سوالات زیر پاسخ دهید:

الف) ضعیف ترین و قویترین الگوریتم رمزنگاری و امضای پیشنهاد شده توسط کلاینت در اولین نشست چیست؟ دلیل انتخاب خود را ذکر کنید.

ب) در اولین نشست سرور کدام الگوریتم رمزنگاری را انتخاب کرده است؟

پ) نام شرکت صادر کننده گواهی نامه ی سرور چیست؟

ت) با کلید خصوصی داده شده پیام Finished در پایان فاز Handshake را رمزگشایی کنید این پیام شامل چه مقادیری است. و ارسال آن چگونه از حمله مرد میانی جلوگیری میکند؟

ث) بسته های شماره ۱۱ و ۲۹ را رمزگشایی کنید این مورد چه ضعفی از RSA را نشان میدهد؟

در مورد ترافیک ضبط شده مربوط به TLSv1.2 به سوالات زیر پاسخ دهید:

ج) دو اتصال بین کلاینت و سرور صورت گرفته است. پیام های تبادل شده در فاز Handshake را بین این دو اتصال مقایسه و بیان کنید کدام یک از پیام ها رمز شده و کدام یک آشکار است.

چ) کلاینت چگونه عملیات برقراری دومین اتصال را کوتاه تر کرده است؟ این کار چگونه به تسریع دریافت اطلاعات از سرور و در نتیجه ی آن بارگذاری سریعتر صفحات وب کمک میکند؟

در مورد ترافیک ضبط شده مربوط به TLSv1.3 به سوالات زیر پاسخ دهید:

ح) در اولین Handshake چرا پیام Client Key Exchange ارسال نشده است؟

خ) بسته ی شماره ۸ حاوی پروتکل Change Cipher Spec است. توضیح دهید این پیام به چه

معناست و کلاینت چگونه قبل از دریافت پاسخ سرور مبنی بر توافق روی کلید محتوای رمز شده فرستاده است؟

د) آیا مشابه TLSv1.2 میتوان بدون رمزگشایی پیام ها گواهی نامه ی سرور و مقدار شناساگر نشست را یافت؟

ذ) با مقادیر محرمانه ی ارائه شده پیام ها را رمزگشایی کرده و شناسه ی استفاده شده برای ادامه ی نشست و همچنین پیامی که در آن سرور و کلاینت این مقدار را تبادل کرده اند مشخص کنید.

ملاحظات تمرین

مهلت تحویل: ۲۴ خردادماه

- تمرین‌ها به صورت انفرادی انجام می‌شوند.
- لطفا پاسخ خود را در قالب یک فایل PDF با فرمت زیر در سامانه Elearn بارگذاری کنید:

StudentID_Lastname_HW4

- امکان ارسال تمرین نهایتاً با دو روز تاخیر با کسر ۱۰ درصد نمره به ازای هر روز وجود دارد.
- در صورت استفاده از منابعی غیر از کتاب مرجع در انجام تمرین، لطفاً حتماً نام منبع خود را ذکر کنید. در صورت مشاهده شباهت غیرمعمول میان پاسخ‌های دو نفر یا در صورتی که پاسخ‌ها برابر با محتوای منابعی غیر از کتاب مرجع باشد و نام منابع مورد استفاده ذکر نشده باشد، نمره‌ای برای شما منظور نخواهد شد.

موفق باشید!