۱. کد مربوط به یک صفحه وب آسیب‌پذیر به شما داده شده است. این صفحه وب را به‌صورت محلی اجرا کنید و چالش‌های زیر را حل کنید (۲۵ نمره):

- دو چالش XSS در پوشه xss وجود دارد. با ورودی‌های مناسب حمله‌ای انجام دهید که یک پیغام حمله موفقیت‌آمیز در صفحه نمایش داده شود (مثلاً به کمک alert). ورودی منجر به حمله را در گزارش خود بیاورید.
- یک چالش SQL Injection در پوشه sqli وجود دارد. در این صفحه یک فرم ورود به حساب کاربری وجود دارد. یک رشته ورودی بسازید که بدون نیاز به نام کاربری و رمز عبور پیغام ورود موفقیت‌آمیز را دریافت کنید. ورودی منجر به حمله را در گزارش خود بیاورید.
- کدها را به‌صورتی تغییر دهید که آسیب‌پذیری‌های دو قسمت اول رفع شود. توضیح دهید که چرا آسیب پذیری ها رفع شده است و کدهای تصحیح شده را در یک فولدر به نام Patched همراه با گزارش خود ارسال کنید.

۲. در درس با کنترل دسترسی اختیاری در سیستم‌عامل ویندوز آشنا شدید. در این سؤال با کنترل دسترسی اجباری در این سیستم‌عامل آشنا خواهید شد (۲۰ نمره).

در سیستم‌عامل ویندوز سیستمی با نام Windows Integrity Levels و یا WIL وجود دارد که تا حدی می‌تواند مدل کنترل دسترسی مبتنی بر صحت را برای ما فراهم کند. برای استفاده از این سیستم و تنظیم برچسب صحت فایل‌ها و برنامه‌ها، از ابزاری به نام chml استفاده کنید. این برنامه در فایل‌های ارسالی ضمیمه شده است.

- یک فایل متنی بسازید و متنی را در آن قرار دهید.
- حال سطح صحت این فایل را در سطح high قرار دهید و از آن بخوانید و در آن بنویسید. چه اتفاقی می‌افتد؟ با ذکر دلیل توضیح دهید.
- اکنون سیاست No Read Up را برای این فایل تنظیم کنید و مرحله دوم را تکرار کنید و اتفاقی که رخ می‌دهد را به همراه ذکر دلیل گزارش کنید.
- برنامه‌ای به زبان C/C++ بنویسید که فایل قسمت اول را خوانده و محتوای آن را چاپ کند و سپس سعی کنید در فایل چیزی بنویسید. چنان چه هر کدام از عملیات فوق ممکن نبود کد بایستی با صدور خطای مناسب کاربر را آگاه سازد. این فایل را کامپایل کرده و فایل exe آن را برای قسمت بعد به دست بیاورید. کد خود را به همراه گزارش ارسال کنید.
- سطح صحت فایل متنی را در سطح medium گذاشته و سطح صحت برنامه نوشته‌شده را در سطح low قرار دهید و قسمت دوم و سوم را با استفاده از برنامه‌ای که نوشتید دوباره انجام دهید و نتایج را گزارش کنید.
- این سیستم در قبال جریان بالا به پایین (یعنی خواندن از یا نوشتن در سطح پایین‌تر) چه سیاستی را دنبال می‌کند؟

۳. در این سؤال به پیاده‌سازی کنترل دسترسی در یک پایگاه داده می‌پردازید. برای حل این سؤال می‌توانید از هر DBMS مبتنی بر SQL استفاده کنید. پایگاه داده یک بیمارستان را در نظر بگیرید که از چهار جدول تشکیل شده است (۳۵ نمره):

- جدول اطلاعات پزشکان (شامل نام پزشکان، تخصص پزشکان، شماره تماس، کد ملی)
- جدول اطلاعات بیماران (شامل نام بیماران و بیماری آن‌ها، شماره تماس، کد ملی)
- جدول بیماری بیماران (شامل کد ملی بیمار و نام بیماری)
- جدول معاینات انجام‌شده روی بیماران (شامل نام بیمار، بیماری و نام پزشک)

ابتدا چهار جدول ذکرشده را بسازید. می‌توانید اطلاعاتی را علاوه بر ستون‌های ذکرشده به‌صورت دلخواه برای جداول تعریف کنید. سپس:

- سه نقش در نظر بگیرید: کاربر عادی (Normal User)، پرستار (Nurse) و پزشک (Physician). این سه نقش را در پایگاه داده تعریف کنید و یک کاربر برای هر نقش در نظر بگیرید.
- قواعد کنترل دسترسی را به‌صورت تعریف کنید که خواسته‌های زیر برآورده شود:
  - کاربر عادی فقط حق خواندن نام پزشکان و تخصص آن‌ها را دارید.
  - پزشکان حق خواندن و به‌روزرسانی جدول بیماران و بیماری‌ها را دارند ولی حق ایجاد و حذف ندارند.
  - پرستاران تمامی دسترسی‌ها روی داده‌های جدول معاینات، جدول بیماری‌ها و جدول بیماران را دارند. پرستاران همچنین دسترسی خواندن اطلاعات پزشکان را دارند ولی دسترسی ایجاد، به‌روزرسانی و حذف آن‌ها را ندارند.
- با دستورات مناسب برای کاربران ساخته‌شده با نقش‌های ذکرشده، برقراری سیاست‌های ذکرشده را نشان دهید.

۴. هدف از این سؤال آشنایی شما با فایروال iptables است (۲۰ نمره).

بخش اول: عملی

iptables را در سیستم خود نصب کنید.

- قانونی بنویسید که ترافیک خروجی ICMP را drop کند.
- قانونی بنویسید که همه ترافیک ورودی به‌جز ترافیک SSH را allow کند.
- قانونی بنویسید که همه ترافیک ورودی از یک آدرس آی پی مشخص (آدرس ماشین مجازی خودتان) را reject کند.

برای تست درستی قوانینی که نوشته‌اید می‌توانید از یک ماشین مجازی استفاده کنید. از این تست ها اسکرین شات گرفته و به همراه توضیح در پاسخ خود بیاورید.

بخش دوم:

- قانونی بنویسید که همه ترافیک ورودی SSH به‌جز از شبکه 192.168.1.0/24 را allow می‌کند.
- قانونی بنویسید که همه ترافیک ورودی به‌جز ترافیکی که مربوط به یک اتصال[1] است، را reject کند.
- قانونی بنویسید که همه ترافیک ورودی TCP روی پورت ۸۰ را به آدرس دیگری فوروارد کند.
- قانونی بنویسید که همه ترافیک ورودی به پورت ۸۰ را به پورت ۸۰۸۰ فوروارد کند.
- قانونی بنویسید که به جلوگیری از حملات منع سرویس در یک وب سرور کمک کند.

[1] Established connection

نکات مهم

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

DNS-HW4-STDID.zip..... (STDID شماره دانشجویی شماست)
- DNS-HW4-STDID.pdf
- Q1
  - Patched
- Q2
  - Code.c/Code.cpp

- اطمینان حاصل کنید که سند آشنایی با مقررات تمرین‌ها را به‌خوبی مطالعه کرده و نسبت به نکات و دلایل احتمالی کسر نمره ذکرشده در آن آگاهی کامل را به دست آورده‌اید.
- پاسخ تمرین باید به‌صورت تایپ شده و مرتب (با مرزبندی مشخص برای هر سؤال) باشد.
- پاسخ هر سؤال باید دقیق و متناسب با سؤال باشد. از ذکر مطالب مبهم، نامرتبط و زائد خودداری کنید.
- در صورت استفاده از هرگونه منبع برای پاسخ به سؤالات، ذکر اسم و نشانی دقیق و کامل دسترسی به صفحه موردنظر الزامی است.