بسمه تعالی

دانشگاه صنعتی امیرکبیر، دانشکده مهندسی کامپیوتر

امنیت اطلاعات و ارتباطات

نمونه آزمون پایانی- زمان: ۹۰ دقیقه

مدرس: حمیدرضا شهریاری

۹۴/۱۰/۱۵

نام: ..... شماره دانشجویی: .....

پرسش	۱	۲	۳	۴	جمع
بارم	۹	۱۶	۱۵	۸	۴۸
نمره					

توجه:

- آزمون کتاب و جزوه بسته است.
- استفاده از هر گونه وسایل محاسباتی و ارتباطی (مانند لپ تاپ، موبایل، تبلت و غیره) ممنوع است.
- ابتدا همه سوالها را مرور نمایید و اگر ابهامی در سوال وجود دارد، در همان ۱۰ دقیقه اول بپرسید.
- سوالها را با همان فرضیات داده شده حل کنید. در صورتی که فرض جدیدی لازم است، صریحاً بنویسید.

---

۱. [۹نمره] هر یک از مفاهیم زیر را تعریف کنید:

(آ) Computer Worm

.....

(ب) Rootkit

.....

(ج) Flase Positive Error

.....

۲. [۱۶نمره] درباره تهدیدهای زیر مشخص کنید که پروتکل SSL آیا می‌تواند با آن مقابله کند یا خیر و چگونه؟ یعنی در صورتی که مقابله می‌کند توضیح دهید با چه ویژگی از حمله جلوگیری می‌کند یا آن را مشکل‌تر می‌سازد.

(آ) حمله شنود بسته های IP

(ب) حمله تحلیل ترافیک بسته های IP

(ج) حمله مردی در میانه

(د) شنود گذرواژه فرم وب

(هـ) حمله SYN FLooding

۳. سیستم احراز هویت در سیستم عامل اندروید به صورت ترسیم یک خط شکسته حاصل از اتصال حداکثر ۹ نقطه است که به صورت یک مربع چیده شده‌اند. برای سادگی فرض کنید نقاط روی یک دایره چیده شده‌اند و یک الگوی گذرواژه به صورت یک خط شکسته شامل حداقل دو نقطه پیوسته است که ترتیب نقاط مهم بوده و نقاط تکراری در الگو وجود ندارد. مدیر سیستم مایل است هنگامی که احتمال حدس گذرواژه‌ها به ۰.۱ رسید، آنها را منقضی نماید. زمان مورد انتظار برای رسیدن به این احتمال را تعیین نمایید، اگر:

(آ) [۷نمره] در هر ثانیه بتوان یک گذرواژه را تست کرد.

(ب) [۸نمره] در هر ثانیه بتوان یک گذرواژه را تست کرد و در هر ۵ بار تست سیستم ۳۰ ثانیه تاخیر ایجاد می‌کند.

۴. (آ) [۲نمره] فایروال چیست؟

.....

(ب) [۲نمره] امکان NAT در فایروال را توضیح دهید.

.....
.....
.....
.....

(ج) [۴نمره] آیا استفاده از NAT تاثیری در پروتکل SSL دارد؟

.....
.....
.....
.....