۱- عبارت "security" را با کمک تکنیک Radix-64 کد کنید. فرض کنید هر کاراکتر به صورت کد اسکی ۸ بیتی ذخیره شده اند. (از جدول کد گذاری radix 64 در صفحه ۲۶۷ نسخه ۴ کتاب استالینگز کمک بگیرید).

۲- در فاز اول SSL handshake، پیغام های Hello و اعلام توانایی پشتیبانی الگوریتم های مختلف رمز نگاری، به صورت plaintext رد و بدل می شود. حمله کننده می تواند این پیغام ها را شنود کند و آن ها را تغییر دهد، برای مثال به پروتکل های ضعیف تر نسبت به چیزی که دو طرف مشخص کرده اند. فرض کنید که از میان server و client ، تنها server یک certificate دارد. آیا مسئله فوق مشکلی در روند امنیت پروتکل SSL handshake ایجاد می کند؟ با شرح جزییات توضیح دهید. (برای خواندن جزییات بیشتر از پروتکل SSL handshake ، حتما به کتاب درسی تان مراجعه کنید)

۳- دو کامپیوتر داریم که در دو شبکه LAN متفاوت نشسته اند. در حالتهای زیر بگویید از کدام یک از مود های IPSec میتوان برای امن سازی ارتباط آنها استفاده کرد.

الف) هر دو کامپیوتر ها و روتر هایی که LAN آنها را به اینترنت متصل میکنند IPSec را پیاده سازی کرده اند.
ب) تنها یک کامپیوتر و هر دو روتر هایی که LAN ها را به اینترنت متصل میکنند IPSec را پیاده سازی کرده اند.
ج) تنها روتر هایی که LAN ها را به اینترنت متصل میکنند IPSec را پیاده سازی کرده اند.
د) آیا مود IPSec به اینکه چه پروتکلی از میان ESP و یا AH قابل استفاده بشود ارتباطی دارد؟

۴- استاندارد IPSec بیان میکند که اگر در مود Transport دو SA از نوع ESP و AH بخواهند باهم استفاده شوند، یک ترتیب بر دیگری ارجهیت دارد: یعنی ابتدا باید پروتکل ESP اعمال شود و سپس پروتکل AH. بنظر شما چرا این ترتیب در استاندارد توصیه شده است؟

۵- در مبحث firewalling، یک نیاز مدیریتی از دیدگاه امنیت اینست: "همه ترافیک رد و بدل شده Web با بیرون باید از طریق پروکسی Web سازمان صورت پذیرید". هرچند این درخواست معقولی است اما اجرای آن سخت تر از حرف زدن در مورد آنست. توضیح دهید که چرا این کار مشکل است (هنگام پاسخگویی درنظر داشته باشید که ترافیک Web از چه چیزهایی تشکیل شده است و چگونه میتوان بر آن نظارت کرد. طیف پورتهای مورد استفاده توسط پروتکل های مختلف و سرور ها و browser ها را هم در نظر داشته باشید).

۶- فرض کنید که از شما خواسته میشود که برای سیاستهای زیر، در یک Firewall ای مانند آنچه در شکل 11.3 کتابتان آمده است Rule های لازم را اعمال کنید. مجموعه Rule های لازم را در دو جدول (مشابه جدول نمونه داده شده) برای External Firewall و Internal Firewall بنویسید (میتوانید بجای آدرس ها و پورت ها، اسامی را بنویسید).

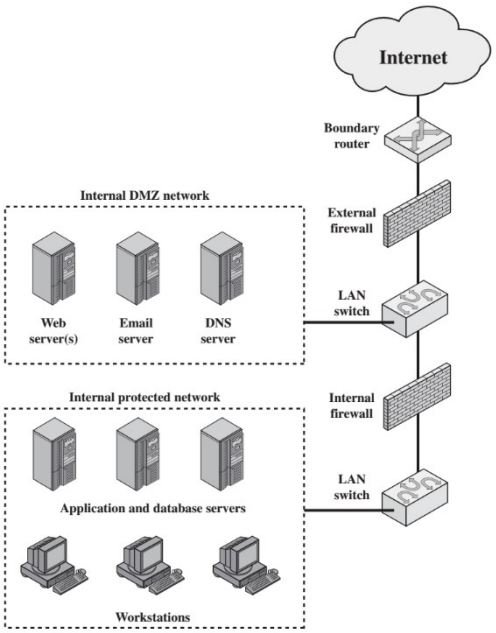

Figure 11.3 Example Firewall Configuration

a) کاربران داخلی بتوانند صفحه Web سازمان را مشاهده کنند و همینطور کاربران اینترنت. اما کاربران داخلی نباید بتوانند به اینترنت دسترسی داشته باشند و کاربران اینترنتی نیز نباید به شبکه داخلی دسترسی پیدا کنند.

b) علاوه بر موارد فوق، کاربران داخلی بتوانند از طریق سرور ایمیل سازمان با SMTP ایمیل بفرستند. دریافت ایمیل آنها باید از طریق یک outlook و با پروتکل pop3 باشد.

۷- یکی از ضعفهای WEP استفاده از CRC بجای hash برای مقصود دست نخوردگی است.

a) ثابت کنید که CRC یک تابع خطی از ورودی است.

b) اگر سه بسته با IV یکسان بدست شما بیفتد، نشان دهید که با استفاده از خاصیت فوق چگونه سرویس امنیتی integrity را میتوان خدشه دار کرد و بسته ای موثق ساخت.

۸- در استاندارد IEEE 802.11 اولیه، مکانیزم Open System Authentication تنها دو مرحله داشت. یک درخواست Authentication توسط Client که شامل ID وی (معمولا MAC address) است ارسال میشود. اگر این آدرس در لیست آدرسهای سیاه AP نبود (و یا در لیست ایستگاههای مجاز بود) ، پیام Authentication Successful را پس میفرستد (در غیر اینصورت Authentication Failure میفرستد). بنظر شما مشکل این روش هم از دید امنیتی و هم از بعد عملی در دنیای واقعی با تعداد زیادی AP چیست؟

۹- مشخص کنید هر کدام از دو قطعه کد زیر چه نوع بد افزاری را نشان می دهند.

```
legitimate code
if data is Friday the 13th;
    crash_computer();
legitimate code
```

```
username = read_username();
password = read_password();
if username is "133t h4ck0r"
    return ALLOW_LOGIN;
if username and password are valid
    return ALLOW_LOGIN
else return DENY_LOGIN
```