آزمایشگاه امنیت شبکه

DoS, DDoS

مقدمه: در این آزمایش قصد بر آن است که دانشجویان با حملات منع سرویس آشنا شوند.

آزمایش ۵-۱: حمله SYN Flooding

- یک حمله Syn Flooding انجام دهید.
- با استفاده از بررسی بسته‌ها در وایرشارک درستی حمله خود را ثابت کنید.

آزمایش ۵-۲: حمله IP Spoofing

- یک مولفه با آدرس IP مثلا A در نظر بگیرید (مثلا آدرس کامپیوتر حمله کننده)
- یک حمله جعل آدرس IP انجام دهید.
- یک کرنل ماژول برای لینوکس بنویسید که ترافیک از سمت آدرس A و ۹ آدرس بعـــدی از آدرس A را بلاک کند. حال با استفاده از همان ماشین A حمله SYN Flood را انجام دهید.

آزمایش ۵-۳: حمله Mitnick

- این حمله را توضیح دهید و تفاوت آن با حمله man in the middle را ذکر کنید.
- یک حمله Mitnick علیه برنامه کلاینت-سروری که در جلسه اول نوشتیم انجام دهید.

آزمایش ۵-۴: DDoS

- برنامه ای بنویسید که عملیات SYN Flooding علیه ماشین قربانی را انجام دهد.
- این برنامه را بر روی حداقل دو ماشین (حمله) نگهداری کنید.
- ماشین سومی را به عنوان قربانی در نظر بگیرید.
- به دو ماشین حمله دستور اجرای همزمان برنامه را دهید.
- نتیجه را تحلیل کنید.